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

Which of the following shell command can be used to check disk usage in a Linux OS ECS

A. Df –h
B. Echo
C. Free –m
D. Ps –e –o

Answer: A

Question: 2

Which of the following application vulnerabilities are not as popular as others?

A. SQL Injection
B. XSS exploit
C. File uploading vulnerability
D. Kernel privilege breaking

Answer: D

Question: 3

In a regular server maintenance operation, the purpose of installing a patch on the operating system is?

A. To improve server resource usage
B. to improve system usability
C. to enhance system functionality
D. to avoid existing system vulnerabilities being used by some hackers

Answer: D

Question: 4

Which of the following statements is NOT true about web application security protection best practices?

A. enforce security management to any public service
B. keep installing official released patches will be good enough
C. keep monitoring system processes , performance and status
D. always scan input by user through web application

Answer: B

Question: 5

Which of the following function is provided by 'server guard' patch management service?

A. fix vulnerability found in open source software using Alibaba self-developed patch
B. detect any vulnerability before it bursts
C. release official patches for any exposed vulnerability
D. stop hacker's vulnerabilities probing

Answer: B

Question: 6

In May 2017 a new blackmail virus WannaCry burst globally, using Windows OS open port 445 to initiate its attacks. What is the quickest way to prevent this kind of attacks?

A. disable port 445
B. set a highly complexed administrator password
C. encrypt all data on server side
D. put sensitive data in some hidden directory

Answer: A

Question: 7

Which of the following function is NOT provided by 'Server Guard' vulnerability detection?

A. Trojan detection
B. weak password detection
C. sensitive data encryption
D. Linux system vulnerability scanning

Answer: C

Question: 8

Reliable server daily operation and security management are essential for continuous service running. Which of the following statement is NOT correct regarding to this scenario?

A. set easy to remember password to help administrator quickly login and solve problems
B. patch system timely and frequently
C. enable build-in OS firewall and configure it properly
D. disable the ports which are not providing service anymore

Answer: A

Question: 9

Which of the following statements is the possible reason that might lead to system vulnerabilities?

A. software logic flaw or mistakes made during software development cycle
B. hardware devices are not up to date

C. system administrator didn't follow the operation manual exactly
D. The proprietary software that is safer than open source one should be installed

Answer: A

Question: 10

Which command in Redhat Linux shell can be used to check if some specific string is included in a bunch of text files?

A. Watch
B. Find
C. Grep
D. Ca

Answer: C

Question: 11

In Windows OS which command can be used to track IP route, including involved node and spent time on each hop?

A. Wroute
B. Route
C. Tracert
D. Traceroute

Answer: C

Question: 12

Which command in Windows OS can be used to open a terminal?

A. Painter.exe
B. Cmd.exe
C. Batch.exe
D. Term.exe

Answer: B

Question: 13

Which of the following protocol is dedicated to resolve IP and MAC addresses?

A. TCP

B. ARP
C. DNS
D. ICMP

Answer: B

Question: 14

Which web server is default one in Windows OS?

A. HTTPD
B. IIS
C. Web Daemon
D. Apache

Answer: B

Question: 15

For an IP subnet like 192.168.0.0/24, which of the following statements is true?

A. Every IP address inside this subnet can be assigned as a HOST IP
B. The broadcast address of this subnet is 192.168.0.0
C. The network address of this subnet is 192.168.0.255
D. IP communication between the hosts inside this subnet will not go through the gateway

Answer: D

Question: 16

In Windows OS what command can be used to open registry table and edit it?

A. Gpedit
B. Regedit
C. Gedit
D. Zedit

Answer: B

Question: 17

What status transition flow a TCP client will go through in order to proactively establish connection and disconnect it?

A. SYNC_SENT- ->ESTABLISHED-->FIN_WAIT1-->FIN_WAIT2-->TIME_WAIT

B. SYNC_SENT- ->ESTABLISHED-->FIN_WAIT1-->FIN_WAIT2-->CLOSE_WAIT
C. SYNC_RCVD- ->ESTABLISHED-->CLOSE_WAIT-->TIME_WAIT-->LAST_ACK
D. SYNC_SENT- ->SYNC_RCVD-->ESTABLISHED-->FIN_WAIT1-->FIN_WAIT2

Answer: A

Question: 18

Which of the following protocol can be considered as 'application' layer protocol in ISO/OSI 7 layer model?

A. TCP
B. UDP
C. IP
D. SMTP

Answer: D

Question: 19

Which of the following HTTP status code does reflect that the requested page does not exist?

A. 403
B. 404
C. 201
D. 304

Answer: B

Question: 20

In Windows OS users can set software update configuration in various modes. Which software update configuration listed here is not supported at all?

A. Set a fixed upgrade schedule
B. Automatically install any upgrade if available
C. Always ask for user's permission before installation
D. never check for upgrade

Answer: D

Question: 21

Which of the following statements are NOT true about 'Server Guard' remote logon detection functionality?

A. It needs to setup common logon location in 'Server Guard' configuration
B. It can detect the attacking tool used by attacker

C. It can detect the remote logon used source IP address

D. It can send warning message to 'Server Guard' user

Answer: B

Question: 22

Which of the following functions does not belong to what WAF can provide?

A. DB encryption

B. SQL injection detection

C. XSS attack detection

D. unauthorized resource access blocking

Answer: A

Question: 23

After using WAF, if you find there are many user input data in the network traffic, you should apply:

A. Loose protection policy

B. Normal protection policy

C. Strict protection policy

D. Progression protection policy

Answer: C

Question: 24

After WAF was purchased, users need to add one DNS record to map their domain name to WAF provided IP. What is the type of that DNS record?

A. A record

B. CNAME Record

C. TXT Record

D. MX Record

Answer: B

Question: 25

From which of the following attacks WAF will not provide protection?

A. SYN Flood

B. Web Server vulnerability attack

C. Core files unauthorized access

D. HTTP Flood

Answer: A

Question: 26

Which of the following security vulnerability is not a 'Server Side' security issue?

A. SQL injection
B. System Command Execution vulnerability
C. CSRF(cross site request fraud)vulnerability
D. File uploading vulnerability

Answer: C

Question: 27

Which of following statements is NOT true about anti-DDOS basics and anti-DDOS Pro?

A. both can defend DDOS attack
B. anti-DDOS pro is free to charge
C. anti-DDOS pro has more capabilities to defend against DDOS attacks
D. anti-DDOS pro can protect both inside and outside Alibaba Cloud servers

Answer: B, D

Question: 28

Which of the following statements is TRUE about Anti-DDOS basics?

A. it can only protect servers outside of Alibaba Cloud
B. it is free to charge
C. need to turn on manually
D. There is no service limitation for peak traffic

Answer: B

Question: 29

What will the correct stops the traffic will flow through if the user used all following cloud service: WAF, Anti-DDOS pro, CDN.

A. CDN- >Anti-DDOS Pro->WAF->Original Website
B. Anti-DDOS Pro->CDN->WAF->Original website
C. CDN- >WAF->Anti-DDOS Pro->Original website
D. Anti-DDOS Pro->WAF->CDN->Original website

Answer: B

Question: 30

If your company's official website is tampered, the consequence of such attack could NOTbe:

A. Website is used for some illegal attempts
B. Public image or reputation of your company is damaged
C. Business is impacted
D. Physical server is damaged

Answer: D

Question: 31

If WAF service user updated web page content after turning on website tampering protection, what does user need to do on WAF console?

A. Update cache
B. turn on protection switch manually
C. add one protection rule
D. restart the whole WAF service

Answer: A

Question: 32

Which of the following methods can't be used to prevent SQL injection attack?

A. Strict input check
B. Use secured function call

C. SQL precompiling and variable binding D. Warning message for abnormal input

Answer: D

Question: 33

Which of the following protocols is not an application level protocol in ISO/OSI 7 layer networking model?

A. FTP
B. TCP
C. HTTP
D. SNMP

Answer: B

Question: 34

Which of the following statements is true about classic network and VPC?

A. they can do same thing
B. you can customize your private IP in a classic network
C. you can customize your private IP in VPC
D. servers inside VPC can only communicate to other VPC network

Answer: A

Question: 35

Which of the following statements is NOT true about EIP and NAT gateway?

A. NAT gateway can support multi servers inside VPC to access public internet through one public IP
B. EIP can be bind to different ECS servers at the same time
C. Different EIP can't share bandwidth
D. NAT gateway can support shared bandwidth between several ips

Answer: B

Question: 36

Which of the following products is designed to provide secured and stable network connection among different VPCs?

A. ECS
B. SLB
C. Security Group
D. Express Connect

Answer: D

Question: 37

Which of the following reasons is the least possible reason leading to a network attack?

A. technical skills show off of hacker
B. business competition
C. blackmail
D. help to find system vulnerability

Answer: D

Question: 38

Which of the following options does not belong to 5 key elements of network communication?

A. Encryption Algorism
B. Source IP
C. Destination IP
D. Communication Protocol

Answer: A

Question: 39

What design flaw of TCP/IP protocol does SYN flood attack use?

A. UDP stateless connectio
B. DNS 3 times hands shake
C. TCP 3 times hands shake
D. HTTP plain text transmission

Answer: C

Question: 40

Customer who bought ECS server doesn't need to worry about :

A. Cloud infrastructure security
B. OS vulnerability inside ECS
C. Web service security inside ECS
D. ECS security group setting

Answer: A

Question: 41

Using ECS security group can help you achieve:

A. better CPU usage
B. fine grained access control to you server
C. enlarge your network bandwidth
D. apply QOS to a specific IP

Answer: B

Question: 42

Which of the following functions can be provided by Alibaba Cloud Server Guard product?(the number of correct answers: 3)

A. brute Force password hacking detection and defense
B. suspicious remote login detection and warning
C. security vulnerability scanning and patching
D. anti-ddos
E. anti SQL injection

Answer: A, B, C

Question: 43

When we talk about 'security vulnerability' of ECS server, we are referring to: (the number of correct answers: 3)

A. OS vulnerability
B. Hardware fault
C. Application Vulnerability
D. Hypervisor Vulnerability
E. Data Center Serviceability

Answer: A, C, D

Question: 44

Inside cloud, hypervisor vulnerability could cause the following possible consequences: (the number of correct answers: 3)

A. One client host can access another client's data
B. User service become unavailable
C. Hacker can access host server directly
D. Incorrect client resource usage calculating

Answer: A, B, C

Question: 45

. In the ISO/OSI 7 layers networking model, which of the following functions are provided for the 'network layer'? (the number of correct answers: 2)

A. Routing
B. congestion handling
C. end to end reliable and transparent data transition
D. physical connection

Answer: A, B

Question: 46

If Server Guard (product provided by Alibaba Cloud) report some brute force password hacking attacks, the reporting information will include ? (the number of correct answers: 3)

A. Attack initiated time
B. Attack type
C. Tools attacker used
D. Attack source IP
E. Physical location of attacker

Answer: A, B, D

Question: 47

Which of the following statements about HTTP protocol are true?(the number of correct answers: 2

A. HTTP protocol support state keeping
B. HTTP is based on TCP/IP protocol
C. HTTP request supports methods like: GET, POST, PUT, HEAD, etc.
D. Response code 200 in HTTP protocol means exception on server side

Answer: B, C

Question: 48

Which of the following statements is true about HTTP protocol?
Score 2

A. HTTP is a network layer protocol
B. the data transmitted by this protocol is auto-encrypted
C. default service port is 80
D. HTTP protocol can't be used to transmit file

Answer: C

Question: 49

Which of following elements are included in a TCP/IP based route table ? (the number of correct

answers: 3)

A. Network Destination
B. Netmask
C. Mac Address
D. Gateway IP
E. Port

Answer: A, B, D

Question: 50

Which of the following statements about IPV6 and IPV4 are true?(the number of correct answers: 2)

A. IPV6 has bigger route table size
B. IPV6 address length upper limit is 128 bits
C. IPV6 has more simplified header
D. No network switch device is needed when using IPV6 protocol to transfer data

Answer: B, C

Question: 51

Which of the following logs can be accessed through ECS logs provided by Alibaba Cloud? (the number of correct answers: 2)

A. OS system log
B. Application log
C. Hypervisor log
D. Cloud platform log

Answer: A, B

Question: 52

Which of the following statements are true about the difference between HTTP and HTTPS ? (the number of correct answers: 2)

A. HTTP must use port 80 and HTTPS must use port 443 to provide service
B. HTTPS is more secure than HTTP regarding the way they transfer data
C. Data transferred through HTTPs is under encryption
D. You must buy commercial CA before you setup your own web server with HTTPS service

Answer: B, C

Question: 53

Which of the following protection rules are provided by WAF to better protect from CC attack? (the number of correct answers: 2)

A. Loose
B. Strict
C. Normal
D. Emergency

Answer: A, B

Question: 54

CC customized protection rule supports you to define customized configuration setting.
Which of following items can be self-defined? (the number of correct answers: 3)

A. Source IP
B. URI
C. How long the detection should last
D. How frequently the page is visited by one single source IP
E. Target IP

Answer: B, C, D

Question: 55

Which of the following statements are true to describe a SQL attack commonly used pattern? (the

number of correct answers: 3)

A. Adding more search request together with the original one
B. adding an absolute true condition to bypass original request
C. use incorrect SQL function
D. use selfmade variable
E. adding ";" or "--" to change the original request purpose with new request attached

Answer: A, B, D

Question: 56

Which of the following scenarios are suitable to use CC emergency mode protection? (the number of correct answers: 2)

A. Web page
B. HTML 5 page
C. API
D. Native APPs

Answer: A, B

Question: 57

Which of the following scenarios can be considered as business fraud? (the number of correct answers: 2)

A. massive accounts registration for new user benefits gain
B. data leak because of data transmission with plain text
C. post massive comments with bots to some e-commerce website
D. page content including some porn pictures

Answer: A, C

Question: 58

Which of the following statements about cloud security shared responsibilities model are true? (the number of correct answers: 2)

A. for users who is using IAAS service, they should be responsible for their business system which is on top of cloud infrastructure
B. cloud service provider should guarantee the security of all physical infrastructure
C. the damage caused by attacks leveraging security vulnerability in customers' application server should be charged to cloud service provider
D. cloud user should also take care of some of the hardware maintenance and operation work

Answer: A, B

Question: 59

User A rented 2 ECS server and one RDS in Alibaba Cloud to setup his company public website. After the web site will become available online, the security risks he/she will face will include: (the number of correct answers: 3)

A. physical cable is cut by someone
B. ECS admin password is hacked
C. website codes has some vulnerability
D. RDS DB got unknown remote logon
E. the disk in ECS is broken

Answer: B, C, D

Question: 60

Which of the following scenarios should be handled by anti-DDOS service? (the number of correct answers: 3)

A. Server is under syn flood attack, and is not reachable
B. online game service which is suffering with too many empty connections and slow connections
C. DNS server is under udp flood attack and got no response anymore
D. website is under SQL injection attack
E. website is under XSS attacks

Answer: A, B, C

Question: 61

By default, servers in VPC can't communicate with internet. By implementing which of the following products these servers can gain the capability to communicate with internet? (the number of correct answers: 3)

A. Elastic Public IP
B. CDN
C. EIP + SLB
D. EIP + NAT Gateway
E. DNS service

Answer: A, C, D

Question: 62

Which of the following risks are considered as common network security risk? (the number of correct answers: 2)

A. Massive traffic flood attack
B. Software version is not up to date
C. Data under transferring is being sniffed
D. Physical Fiber Channel Cable is broken

Answer: B, C

Question: 63

Which command in RedHat Linux shell can be used to check disk usage?

A. ls
B. df

C. diskUsage

D. diskSpace

Answer: B

Question: 64

Alibaba Cloud will provide hot fix to address existing vulnerabilities. Which of the following statements is true about this 'hot fix'?

A. hot fix doesn't need to reboot physical host

B. service will not be available during the hot fix

C. hot fix means the host need to reach some temperature upper limit to be able to proceed

D. hot fix is transparent to end user

Answer: A

Question: 65

Which of the following issues would not happen if ECS server is under attack by hackers?

A. sensitive data leak

B. service running on that server is not available

C. physical server damage

D. compromise the reputation of service provider on that server

Answer: C

Question: 66

Which of following statement about 'Server Guard' Trojan scanning functionality is NOT correct?
Score 2

A. Server Guard Agent will automatically scan your web pages directories and look for any webshell file.

B. A change to a file in the web pages directories will trigger a scan for that file

C. you can log on to the Server Guard console to isolate webshell files with one click.

D. Server Guard will delete any suspicious webshell file immediately

My

Answer: B. Other file

says D

Answer: D

Question: 67

Which of the following issues will NOT be an issue anymore using Alibaba Cloud ECS server? Score 2

A. server is under brute force password hacking
B. hardware disk or memory broken
C. infection by Trojan Virus
D. application vulnerability being leveraged by hackers

Answer: B

Question: 68

Which of the following benefit cannot be provided by 'Server Guard' Score 2

A. lower the risk of sensitive data leak
B. improve the usage of system resource
C. lower the cost of security protection
D. get instant alerts after attacks are detected

Answer: B

Question: 69

In Windows OS you can turn off a service through: Score 2

A. Control Panel->Management Tool->Stop the running service
B. Control Panel->windows update->Stop
C. Create new firewall rule to stop service
D. Delete administrator role and related accounts

Answer: A

Question: 70

If your company has a lot of employees who would try to simultaneously access ECS server protected by 'Server Guard' using your company's intranet, the 'Sever Guard' may mistakenly identify those access requests as attacks. Which of the following methods is the best way to solve this problem? Score 2

A. set a highly complexed administrator password
B. change the rule of security group to unblock all company internal ips
C. add those IPs which need to access ECS server into 'Server Guard' logon white list
D. ask employees to access that ECS server not very frequently

Answer: C

Question: 71

Which of the following protocol is dedicated for time sync up? Score 2

A. HTTP
B. ICMP
C. NTP
D. UDP

Answer: C

Question: 72

Which of the following statements about 'webshell' detection feature of WAF is NOT true?

A. It will totally block any file to be able to upload to the web server
B. cache will be enabled only after you turn on the protection switch
C. there is a switch need to be turned on first
D. If you changed some page content, you can use 'cache update' button to manually update the cache

Answer: A

Question: 73

Which of the following statements is NOT true about daily operation on server account

andpassword maintenance?

A. change'Administrator' to some other name
B. with'Server Guard protection In Allbaba Cloud,you can set password to some easy to remember words.
C. except for some necessary accounts for system manogement,.dlsoble or delete other seldomly used accounts
D. always set a complexed passwcwd using combination of numbers,letters and other characters

Answer: B

Question: 74

In Linux OS, if access control to a file is shown as '-rwxrw-r--' in shell command, which of the following statements are true?
Score 2

A. This file is a text file
B. The access privilege of this user group is read only
C. The owner of this file has read/write/execution privilege to this file
D. Other users (outside of this user group) can execute this file

Answer: C

Question: 75

Which service in RedHat Linux OS can be used to build network firewall functionality?
Score 2

A. iptables
B. ipfirewall
C. linuxfw
D. netstat

Answer: A

Question: 76

Which Internet protocol is used to implement Linux shell command 'ping'
Score 2

A. ICMP
B. UDP
C. PING
D. TCP

Answer: A

Question: 77

Which protocol is a 'data link' layer protocol in ISO/OSI 7 layer network model?
Score 2

A. ICMP
B. ARP
C. FTP
D. UDP

Answer: B

Question: 78

In Linux OS, if you want to set a file access privilege to read, write, and execute for the owner only, what octal number will reflect such settings correctly?
Score 2

A. 755
B. 700
C. 777
D. 766

Answer: B

Question: 79

Please list the correct order of the following 4 steps to enable a WAF service : (1) upload HTTPS CA and private key(HTTPS website only) (2) add the domain name that needs to be protected (3) select the original IP address (4) add CNAME DNS record
Score 2

A. 2314
B. 2341
C. 2431
D. 2413

Answer: B

Question: 80

What is the correct action sequence of WAF protection strategy: (1) CC detection (2) Web application attack detection (3) Access control

Score 2

A. 213
B. 312
C. 132
D. 231

Answer: B

Question: 81

Which version of WAF will provide advisor customized protection rule?
Score 2

A. Advanced Version
B. Enterprise Version
C. Ultimate Version
D. Standard Version

Answer: B

Question: 82

For internet communication, to setup the connection and data transition between source and destination, which of the following information you will need ? (the number of correct answers: 3)

Score 1

A. IP address
B. Port
C. Encryption algorism
D. Protocol
E. Router Location

Answer: A, D

Question: 83

Anti-DDOS basic is provided by Alibaba Cloud for free. Which of the following statements about this service are NOT true? (the number of correct answers: 2)
Score 1

A. basic anti-DDOS service can detect attack traffic and migrate them automatically
B. basic anti-DDOS service can protect any server connect to internet
C. no protection upper limit to the rate of attack traffic
D. CC attack protection need to be turned on manually

Answer: A, C

Question: 84

Which of the following service may under anti-DDOS attack?(the number of correct answers: 3)
Score 1

A. servers in VPC only configured with private network
B. any device internet reachable
C. government website
D. public DNS service
E. offline servers

Answer: B, C, D

Question: 85

The Alibaba Cloud WAF protection strategy provides the following: (the number of correct answers: 3)
Score 1

A. Loose
B. Strict
C. Normal
D. Regular
E. Early Warning

Answer: A, B, C

Question: 86

What modes Alibaba Cloud WAF will provide to defend SQL injection? (the number of correct answers: 2)
Score 1

A. Normal Mode
B. Protection Mode
C. Warning Mode
D. Restriction Mode

Answer: B, C

Question: 87

Which of following attacks could serve as a CC attack? (the number of correct answers: 3) Score 1

A. SYN flood
B. ICMP flood
C. One host simulate many IP addresses
D. Attack through agent
E. Zombie network

Answer: C, D, E

Question: 88

You just physically attached one new disk to a Linux server. Before you can write data into that disk with shell command, which of the following steps you have to finish? (the number of correct answers: 4)
Score 1

A. Make Partitions
B. Raw Format
C. Format
D. Mount
E. Create Filesystem

Answer: A C, D, E

Question: 89

Which of the following statements about VLAN are NOT true?(the number of correct answers: 3)
Score 1

A. users in different VLAN can connect each other directly without pre-configuration
B. different VLAN means different physical location of switches
C. VLAN configuration can be done through an TCP/IP router device

D. VIAN can enhance the network security and data isolation

Answer: A, B, C

Question: 90

For MySQL DB, if the records number exceeds one million in one single table, which of the following methods can help you improve querying speed?(the number of correct answers: 2) Score 1

A. setup index for this table

B. use 'group by' to filter information
C. use 'count(*)' to get total record number before query
D. use 'limit N' to limit the number of possible returned records

Answer: A, B

Question: 91

Which of the following statements about the supported way of MySQL DB for backup are true?(the number of correct answers: 2)

A. you can use 'mysqldump' do logical backup
B. you can copy files directly to do physical backup
C. you can use 'binlog' to do real time backup
D. you must stop accessing to DB before you do logical backup

Answer: A, B

Question: 92

Which of following statements about the possible reasons that cause web server vulnerabilities are true? (the number of correct answers: 2)
Score 1

A. Bugs generated during common component development
B. Hardware configuration is not up to date
C. Software used or OS itself contain some logic flaw
D. End user didn't follow the user manual

Answer: A, C

Question: 93

Which of the following statements are true for how to login to different ECS operating system? (the number of correct answers: 2)
Score 1

A. use 'remote desktop connection' for windows
B. use 'ssh' tool for windows
C. use 'remote desktop connection' for Linux
D. use 'ssh' tool for Linux

Answer: A, D

Question: 94

Apart from technical approaches, the proper data security management rules can be applied in daily operations to lower the risk of information leakage. Which of the following risks can be mitigated setting a strong data security management policy for company's employees? Score 2

A. information is sniffed during network transition
B. under http flood attack
C. sensitive information is taken away by former employee
D. email phishing

Answer: A

Question: 95

Which of the following damages can't be caused by a DDOS attack
Score 2

A. DNS service down
B. physical server broken
C. military commander system down
D. web service down

Answer: B

Question: 96

Which of the following items can't be set in ECS security group configuration?
Score 2

A. OS type
B. network interface
C. authorization policy
D. authorization object

Answer: A

Question: 97

Which of the following 4 functions can be achieved through ECS security group configuration?

A. allow specific IP to remote access ECS server
B. make ECS server be able to defend 15Gb/s DDOS attack
C. fix XSS vulnerability
D. assign customized IP address to ECS

Answer: A

Question: 98

CC attacks can cause serious damages. Which of the following statements about CC attack is not correct? Score 2

A. CC attack will simulate real user requests
B. Will consume massive sever side resource
C. CC attack is done on network layer
D. The request generated by CC attack is hard to be distinguished from normal requests

Answer: C

Question: 99

Which of the following scenarios is the one that 'Server Guard' will support for brute force password hacking detection?

A. RDS remote connection
B. ECS server remote logon or inside DB remote logon
C. Windows shared directory access
D. Linux CRM application remote logon

Answer: B

Question: 100

When 'Server Guard' detects remote logon behavior, what information will be shown on 'Server Guard' console?

A. Illegal Logon!
B. Migrated Already!
C. Logon Successfully!
D. Remote Logon Detected!

Answer: D

Question: 101

Which of the following statements about WAF data risk control feature is NOT true?

A. this feature can only used for single page, can't be used to protect the whole domain name
B. WAF need to inject JavaScript piece into all pages under the same protected domain name to decide if the client side is worth to trust
C. direct access URL protected by this feature will have slider verification pop out
D. this feature is not suitable for scenario needs to call API directly

Answer: A

Question: 102

Which of the following options could NOT be the reason that causes website tampering

A. Share password between different users
B. Botnet attack
C. system vulnerability is not fixed in time
D. Wrong security configuration

Answer: B

Question: 103

Which of the following methods can't be used against CC attack?

A. use WAF
B. change HTTP service to HTTPS service
C. resolve domain name to a disguised IP
D. change the service providing port

Answer: B

Question: 104

Which of the following steps is not a valid step for using anti-DDOS pro?

A. configure to be protected domain name
B. add new DNS record
C. change source IP
D. if original server is using its own firewall, then need to add Anti-DDOS pro IP to its white list
E. bind real customer identity to anti-DDOS pro IP

Answer: E

Question: 105

If user is using anti-DDOS Pro service, but the original server has rule to limit access to the client IPs, which of the following actions is the most proper one to take?

A. enable CDN and change anti-DDOS pro IP to CDN address
B. add anti-DDOS pro IP into customer firewall white list
C. disable original server firewall
D. enable SLB for original server

Answer: B

Question: 106

Which of the following products won't be a DDOS attack target?

A. offline backup tape devices
B. enterprise major website
C. router device
D. online banking system

Answer: A

Question: 107

ECS cloud server is one of the service provided by Alibaba Cloud. If it is attacked by some internet hacker, which of the following consequences such attack could cause? (the number of correct answers: 2)

A. Physical Server Damage
B. Leak of customer sensitive data
C. Service running on this ECS become not available
D. The datacenter where the ECS belongs to need to shutdown

Answer: B, C

Question: 108

In order to stop the service provided through a particular port in Windows OS, which of the following methods can be used to achieve this objective? (the number of correct answers: 3)

A. adjust firewall rule
B. adjust local security policy
C. update OS patch
D. stop the service itself
E. stop all guest role access

Answer: A, B, D

Question: 109

What are the advantages of anti-DDOS pro comparing to anti-DDOS basics service? (the number of correct answers: 3)

A. stronger defending attacks capability
B. elastic protection bandwidth
C. no upper limit to the attack traffic need to be handled
D. can do anti-fraud protection
E. can protect IDC outside Alibaba Cloud

Answer: A, B, E

Question: 110

May, 2017. New blackmail virus WannaCry burst globally. This virus leveraged
Windows OS opened port 445 to initiate the attack, so the quickest way to prevent this kind of attack is?

A. Change 'Administrator' to some other name
B. With 'Server Guard' protection in Alibaba Cloud, you can set password to some easy to remember words.
C. Except some necessary accounts for system management, disable or delete other useless accounts
D. Always set password with highly complex combination of number, letter and other characters

Answer: C

Question: 111

Which of the following statements about ECS, VPC, security groups are NOT true? (the number of correct answers: 2)

A. rule setting for security group supports both in and out direction configuration B. default security group rule is safe enough, please don't change it too much C. by default, ECS in different security group can communicate with each other D. one ECS can be in several different security group

Answer: B, C

Question: 112

Which of the IP addresses are private IP addresses? (Correct Answers: 2)

A. 192.169.1.1
B. 172.16.58.14
C. 10.44.10.45
D. 8.8.8.8

Answer: B, C

Question: 113

Each host connecting to internet will face the potential attacks from internet as follows : (the numbers of correct answers : 3)

A. Brute Force password hacking
B. Trojan planting
C. Content Compliance Requirement
D. Vulnerability scanning
E. Lack of storage resource

Answer: A, B, D

Question: 114

Which of the following Keys in HTTP heads are related to cache control? (the number of correct answers: 3)

A. Cache-Control
B. Date
C. Age
D. Expires
E. Host

Answer: C, E

Question: 115

18. in RedHat Linux shell which command can be used to check what file system is mounted and form what disk device it was done?

A. Ppart
B. Fdisk
C. Du
D. mount

Answer: D

Question: 116

Using RAM, Alibaba Cloud users can create and manage user accounts and control the operation permissions these user accounts possess for resources under your account. Which of the following descriptions of a RAM usage scenario is NOT correct?

A. Enterprise sub-account management and permission assignment
B. Resource operation and authorization management between enterprises
C. Temporary authorization management for untrusted client apps
D. Prevention of network attacks on enterprises

Answer: D

Question: 117

In making cloud accounts more secure, which of the following is NOT a guiding principle?

A. Anonymous logins
B. Login verification
C. Account permissions
D. Authorization distribution

Answer: A

Question: 118

Alibaba Cloud offers different security protection plans to different tenant accounts. Which of the following is NOT a security plan offered by Alibaba Cloud?

A. Password-free login
B. Two-factor authentication
C. Phone number binding
D. Phone or email verification for password resetting

Answer: A

Question: 119

Which of the following security issues is considered by the OWASP to be the most dangerous issue facing cloud computing?

A. Injection
B. Account or service flow hijacking
C. Denial of service
D. Multi-tenant isolation failure

Answer: A

Question: 120

In the Alibaba Cloud, which services can satisfy client user identity management requirements?

A. Security group
B. Server Guard
C. Resource Access Management (RAM)
D. Situational awareness

Answer: C

Question: 121

Which of the following descriptions of the shared responsibilities security model is CORRECT?

A. After beginning to use cloud service, the cloud service provider will become responsible for all of the user's security.
B. After beginning to use cloud service, the user and the cloud service provider will be jointly responsible for cloud security, with each responsible for different layers of security.
C. After beginning to use cloud service, users must still take care of physical and environmental security.
D. After beginning to use cloud service, users only need to pay attention to the security of their own apps and data. All other security will be the responsibility of the cloud service provider.

Answer: B

Question: 122

Which of the following options is the top 1 web application security risk based on OWASP 2017 report?

A. XSS Attack
B. Server Information Theft
C. Code Execution
D. SQL Injection

Answer: D

Question: 123

Which of the following methods CANNOT increase account security?

A. Strong password policies

B. Periodically reset the user login passwords
C. Adhere to the minimum authorization principle
D. Unite user management, permission management and resource management into a single management process

Answer: D

Question: 124

Which of the following 2 security risks are not included in OWASP published 2017 Top 10 Web Application Security Risks

A. Cross-Site Request Forgery(CSRF)
B. Cross-Site Scripting(XSS)
C. Unvalidated Redirects and Forwards
D. Injection

Answer: A, C

Question: 125

Security risk may caused by 'Cloud platform', 'ISV' or 'End user', which of the following options are the possible risks may caused by Cloud Platform?

A. Software development cycle is not formalized
B. Security system overall solutions are not complete
C. Administration tools on Cloud Platform may have some flaws
D. Cloud platform console and API may lack of security hardenning

Answer: B, C, D

Question: 126

Regarding the 'Shared Security Responsibilities' on Alibaba Cloud, which of the following options are the responsibilities Cloud user need to take care of ?

A. Data security inside ECS
B. Physical servers water proof
C. Application vulnerabilities
D. ECS network configuration

Answer: A, C, D

Question: 127

Which of the following options can be considered as Data and Application security risks in IT infrastructure

A. Data integrity
B. Data access control
C. Data readiness
D. Data encryption

Answer: A, B, D

Question: 128

Which of the following Alibaba Cloud products need to be considered to use if you want to build an elastic computing cluster to provide web service together and also with dynamic data and static data separately stored

A. ECS
B. SLB
C. RDS
D. OSS
E. KMS

Answer: A, B, C, D

Question: 129

Which of the following cloud services are the most common ones when we talk about different types of Cloud service

A. IaaS
B. PaaS
C. SaaS
D. DaaS

Answer: A, B, C

Question: 130

Which of the following options can be considered as Physical environment security risks in IT infrastructure

A. Room temperature
B. Data encryption
C. Rain
D. Sounder

Answer: A, C, D

Question: 131

You configure a computer to act as a zombie set in order to attack a web server on a specific date. What would this contaminated computer be part of?

A. The computer is part of a DDoS attack
B. The computer is part of a TCP/IP hijacking
C. The computer is part of a spoofing attack
D. The computer is part of a man-in-the-middle attack

Answer: A

Question: 132

A DoS attack that sends a flood of synchronization (SYN) requests and never sends the final acknowledgement (ACK) is typically known as which of the following?

A. Smurf
B. Ping Flood
C. Fraggle
D. SYN flood

Answer: D

Question: 133

Which of the following can be termed as the Denial of Service Attack? Choose the best answer.

A. A computer on your network has crashed
B. Your router is unable to find a destination outside of your network
C. Your Web server has gone into a loop trying to service a client request
D. You keyboard is no longer responding

Answer: C

Question: 134

In an IP (Internet Protocol) spoofing attack, what field of an IP (Internet Protocol) packet does the attacker manipulate?

A. The version field
B. The source address field
C. The source port field
D. The destination address field

Answer: B

Question: 135

Which of these options contains the three basic target categories for a DoS or a DDoS?

A. Resources, printers and storage devices
B. Networks, systems and applications
C. Systems, memory, network access card
D. Network access card, applications, peripheral devices

Answer: B

Question: 136

You are planning on hosting an eCommerce Web server. You are intent on making the server secure against all external attacks possible. Which of the following would be the best way to test your server for its weaknesses? Choose the best answer.

A. Ping to the server
B. Simulate a DDoS attack on that server
C. Simulate a DoS attack on the server
D. Check if all the patches and required antivirus software has been loaded o the server

Answer: B

Question: 137

What type of attack is likely occuring if you see a significant increase in network traffic and users complain that the web server is hung up?

A. MITM
B. DNS spoofing
C. Ping sweep
D. DoS

Answer: D

Question: 138

Identify the attack where the purpose is to stop a workstation or service from functioning?

A. This attack is known as non-repudiation
B. This attack is known as TCP/IP hijacking
C. This attack is known as denial of service (DoS)
D. This attack is known as brute force

Answer: C

Question: 139

Which of the following services can suffer from DDoS attack?

A. Servers in VPC only configured with private network
B. Any device internet reachable
C. Government website
D. Public DNS service
E. Offline servers

Answer: B, C, D

Question: 140

Which of the following protocols will not be used for a SYN Flood attack?

A. UDP
B. TCP
C. IPX/SPX
D. AppleTalk

Answer: A, C, D

Question: 141

Which of the followings are not the reasons for a DDoS attack?

A. Destroying of integrity
B. Destroying of confidentiality
C. Destroying of availability
D. Destroying of business credit

Answer: A, B, D

Question: 142

What of the followings will happen if encounter DoS or DDoS attack?

A. Data received successfully
B. Delay of data reception
C. Slow access web resources
D. unauthorized access control

Answer: B, C

Question: 143

Which of the following DDoS descriptions are correct?

A. In order to get admin password
B. Steal confidential information
C. Causes the target server unable to process legitimate requests
D. If the target server has no vulnerabilities, the remote attack may still succeed.

Answer: C, D

Question: 144

Which directory is the home directory of root user?

A. /home/root
B. /root
C. /
D. /boot

Answer: C

Question: 145

Which commands can be used to reload the operation system? (Correct Answers: 2)

A. reload
B. shutdown
C. init
D. restart

Answer: D

Question: 146

Which of the following statements about cloud security shared responsibilities model are true? (the number of correct answers: 2)

A. for users who is using IAAS service, they should be responsible for their business system which is on top of cloud infrastructure
B. cloud service provider should guarantee the security of all physical infrastructure
C. the damage caused by attacks leveraging security vulnerability in customers' application server should be charged to cloud service provider
D. cloud user should also take care of some of the hardware maintenance and operation work

Answer: CD

Question: 147

If Server Guard (product provided by Alibaba Cloud) report some brute force password hacking attacks, the reporting information will include ? (the number of correct answers: 3)

A. Attack initiated time
B. Attack type
C. Tools attacker used
D. Attack source IP
E. Physical location of attacker

Answer: CDE