CompTIA

SY0-501

CompTIA Security+ Certification Exam

Version: 64.0

[Total Questions: 593]

Web: www.marks4sure.com

Email: support@marks4sure.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@marks4sure.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@marks4sure.com and our technical experts will provide support within 24 hours.

Copyright

Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Exam Pool A	413
Topic 2 : Exam Pool B	158
Topic 3 : Simulations	22
TOTAL	593

Topic 1, Exam Pool A

Question #:1 - (Exam Topic 1)

A technician wants to add wireless guest capabilities to an enterprise wireless network that is currently implementing 802.1X EAP-TLS The guest network must

• Support client Isolation.

• Issue a unique encryption key to each client.

• Allow guests to register using their personal email addresses

Which of the following should the technician implement? (Select TWO),

A. RADIUS Federation

B. Captive portal

C. EAP-PEAP

D. WPA2-PSK

E. A separate guest SSID

F. P12 certicate format

Answer: A B

Question #:2 - (Exam Topic 1)

Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC

B. HTTPS

C. IPSec

D. TLS/SSL

Answer: A

Question #:3 - (Exam Topic 1)

A Chief Security Officer's (CSO's) key priorities are to improve preparation response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.

B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident

C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks

D. Implement application whitelisting and centralized event-log management and perform regular testing and validation of full backups.

Answer: A

Question #:4 - (Exam Topic 1)

A network technician is setting up a new branch for a company. The users at the new branch will need to access resources securely as if they were at ‘the main location. Which of the following networking concepts would BEST accomplish this‘?

A. Virtual network segmentation

B. Physical network segmentation

C. Sits-to-sits VPN

D. Out-of-band access

E. Logical VLANs

Answer: C

Question #:5 - (Exam Topic 1)

A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES

B. AES

C. MD5

D. RSA

Answer: C

Question #:6 - (Exam Topic 1)

A dumpster diver was able 10 retrieve hard drives from a competitor's trash bin. After installing the and hard drives and running common date recovery software. Sensitive information was recovered. In which of the following ways did the competitor apply media sanitation?

A. Pulverizing

B. Degaussing

C. Encrypting

D. Formatting

Answer: B

Question #:7 - (Exam Topic 1)

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.

B. It provides insurance in case of a data breach.

C. It provides complimentary training and certification resources to IT security staff.

D. It certifies the organization can work with foreign entities that require a security clearance.

E. It assures customers that the organization meets security standards.

Answer: E

Question #:8 - (Exam Topic 1)

A security analyst is determining the point of compromise after a company was hacked. The analyst checks the server logs and sees that a user account was logged in at night, and several large compressed files were exfiltrated. The analyst then discovers the user last logged in four years ago and was terminated. Which of the following should the security analyst recommend to prevent this type of attack in the future? (Select TWO).

A. Review and update the firewall settings.

B. Restrict the compromised user account.

C. Disable all user accounts that are not logged in to for 180 days.

D. Enable a login banner prohibiting unauthorized use.

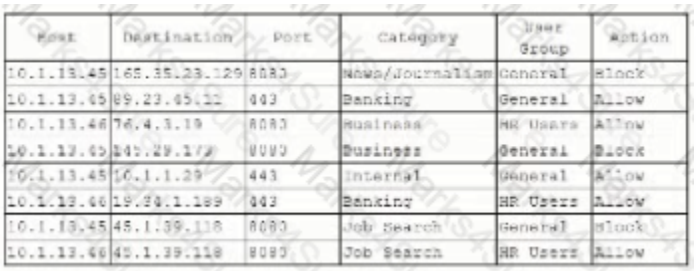
E. Perform an audit of all company user accounts.

F. Create a honeypot to catch the hacker.

Answer: A C

Question #:9 - (Exam Topic 1)

A security analyst investigate a report from an employee in the human resources (HR) department who is issues with Internal access. When the security analyst pull the UTM logs for the IP addresses in the HR group, the following activity is shown:



Host	Destination	Port	Category	User Group	Action
10.1.13.45	165.35.23.129	8080	News/Journalism	General	Block
10.1.13.65	89.23.45.12	443	Banking	General	Allow
10.1.13.46	74.4.3.19	8080	Business	HR Users	Allow
10.1.13.65	141.29.17.8	8080	Business	General	Block
10.1.13.45	10.1.1.29	443	Internal	General	Allow
10.1.13.66	19.84.1.189	443	Banking	HR Users	Allow
10.1.13.45	45.1.39.118	8080	Job Search	General	Block
10.1.13.66	45.1.39.118	8080	Job Search	HR Users	Allow

Which of the following actions should the security analyst take?

A. Ensure the HR employee is in the appropriate user group

B. Allow port 8080 on the UTM for all outgoing traffic

C. Disable the proxy settings on the HR employee's device.

D. Edit the last line Of the ACL On the UTM lo: allow any any.

Answer: A

Question #:10 - (Exam Topic 1)

A penetration tester is testing passively for vulnerabilities on a company's network. Which of the following tools should the penetration tester use? (Select TWO).

A. Zenmap

B. Wireshark

C. Nmap

D. tcpdump

E. Nikto

F. Snort

Answer: B C

Question #:11 - (Exam Topic 1)

An attacker is able to capture the payload for the following packet:

IP 192.168.1.22:2020 10.10.10.5:443

IP 192.166.1.10:1030 10.10.10.1:21

IP 192.168.1.57:5217 10.10.10.1:3389

During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.

B. The application server is also running a web server that has been compromised.

C. The attacker is picking off unencrypted credentials and using those to log in to the secure server.

D. User accounts have been improperly configured to allow single sign-on across multiple servers.

Answer: C

Question #:12 - (Exam Topic 1)

A security engineer needs to obtain a recurring log of changes to system les. The engineer is most concerned with detecting unauthorized changes to system data. Which of the following tools can be used to fulll the requirements that were established by the engineer?

A. TPM

B. Trusted operating system

C. File integrity monitor

D. UEFI

E. FDE

Answer: C

Question #:13 - (Exam Topic 1)

Which of the following should be implemented to stop an attacker from interacting with the hypervisor

through another guest?

A. Containers

B. VM escape protection

C. Security broker

D. Virtual Desktop

Answer: A

Question #:14 - (Exam Topic 1)

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, internet and VoIP services are restored, only to go offline again at random intervals. typically, within four minutes of services being restored. Outages continue throughout the day. impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.

Later that day. the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Select TWO).

A. DOS

B. SSL Stripping

C. Memory leak

D. Race condition

E. Shimming

F. Refactoring

Answer: A B

Question #:15 - (Exam Topic 1)

Which of the following agreement types is a non-contractual agreement between two or more parties and outlines each party's requirements and responsibilities?

A. BPA

B. SLA

C. MOU

D. ISA

Answer: C

Question #:16 - (Exam Topic 1)

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

Answer: C

Question #:17 - (Exam Topic 1)

Which of the following BEST describes why an air gap is a useful security control?

A. It physically isolates two or more networks, therefore helping prevent cross contamination or accidental data spillage.

B. It requires that files be transferred via USB instead of networks that are potentially vulnerable to hacking, therefore preventing virus infections.

C. It requires multiple systems administrators with different credentials, therefore providing separation of duties.

D. It provides physical space between two interlocking doors, therefore providing additional control from unauthorized entry.

Answer: A

Question #:18 - (Exam Topic 1)

A user loses a COPE device. Which of the following should the user do NEXT to protect the data on the device?

A. Call the company help desk to remotely wipe the device.

B. Report the loss to authorities

C. Check with corporate physical security for the device.

D. Identify files that are potentially missing on the device.

Answer: A

Question #:19 - (Exam Topic 1)

A manufacturing company updates a policy that instructs employees not to enter a secure area in groups and requires each employee to swipe their badge to enter the area When employees continue to ignore the policy, a mantrap is installed. Which of the following BEST describe the controls that were implemented to address this issue? (Select TWO).

A. Detective

B. Administrative

C. Deterrent

D. Physical

E. Corrective

Answer: C E

Question #:20 - (Exam Topic 1)

A Chief Information Officer (CIO) is concerned that encryption keys might be exfiltrated by a contractor. The CIO wants to keep control over key visibility and management. Which of the following would be the BEST solution for the CIO to implement?"

A. HSM

B. CA

C. SSH

D. SSL

Answer: A

Question #:21 - (Exam Topic 1)

A coffee company which operates a chain of stores across a large geographical area is deploying tablets to use as point-of-sale devices. A security consultant has been given the following requirements:

• The cashiers must be able to log in to the devices quickly.

• The devices must be compliant with applicable regulations for credit card usage

• The risk or loss or theft of the devices must be minimized

• If devices are lost or stolen, all data must be removed from the device

• The devices must be capable of being managed from a centralized location

Which of the following should the security consultant configure in the MDM policies for the tablets? (Select TWO)

A. Remote wipe

B. Cable locks

C. Screen locks

D. Geofencing

E. GPS tagging

F. Carrier unlocking

Answer: A B

Question #:22 - (Exam Topic 1)

A security engineer implements multiple technical measures to secure an enterprise network. The engineer also works with the Chief information Ofcer (CID) to implement policies to govern user behavior. Which of the following strategies is the security engineer executing?

A. Base lining

B. Mandatory access control

C. Control diversity

D. System hardening

Answer: A

Question #:23 - (Exam Topic 1)

A company Is determining where to host a hot site, and one of the locations Being considered Is In another country. Which of the following should be considered when evaluating this option?

A. Mean RTO

B. Mean RPO

C. Data sovereignty

D. Data destruction laws

E. Backup media recycling policies

Answer: D

Question #:24 - (Exam Topic 1)

Which of the following will ensure the integrity of a file is preserved during the process of forensic acquisition?

A. Compute the hashes for all files and recompute on the destination end.

B. Copy and paste the contents of the acquisition to a secure USB drive.

C. Encrypt the files to an archive to prevent accidental clickers.

D. Use solid state drives to remain reliable and consistent.

Answer: A

Question #:25 - (Exam Topic 1)

An organization is building a new customer services team, and the manager needs to keep the team focused on customer issues and minimize distractions. The users have a specific set of tools installed, which they must use to perform their duties. Other tools are not permitted for compliance and tracking purposes. Team members have access to the Internet for product lookups and to research customer issues. Which of the following should a security engineer employ to fulfill the requirements for the manager?

A. Install a web application firewall.

B. Install HIPS on the team's workstations.

C. Implement containerization on the workstations.

D. Configure whitelisting for the team.

Answer: C

Question #:26 - (Exam Topic 1)

A new network administrator is establishing network circuit monitoring guidelines to catch potentially malicious traffic. The administrator begins monitoring the NetFlow statistics tor the critical Internet circuit and notes the following data after two weeks.

Circuit Name	Min	Max	Avg
Internet	20Mbps	100Mbps	35Mbps

However, after checking the statistics from the weekend following the compiled statistics the administrator notices a spike in traffic to 250Mbps sustained for one hour The administrator is able to track the source of the spike to a server in the DMZ Which of the following is the next BEST course of action the administrator should take?

A. Enable a packet capture on the firewall to catch the raw packets on the next occurrence

B. Consult the NetFlow logs on the NetFlow server to determine what data was being transferred

C. Immediately open a Seventy 1 case with the security analysts to address potential data exfiltration

D. Rerun the baseline data gathering for an additional four weeks and compare the results

Answer: A

Question #:27 - (Exam Topic 1)

A company employee recently retired, and there was a schedule delay because no one was capable of filling the employee's position. Which of the following practices would BEST help to prevent this situation in the future?

A. Mandatory vacation

B. Separation of duties

C. Job rotation

D. Exit interviews

Answer: B

Question #:28 - (Exam Topic 1)

A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices for corporate use must opt in to the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading

B. Full device encryption

C. Application management

D. Containerization

Answer: C

Question #:29 - (Exam Topic 1)

Which of the following BEST explains 'likelihood of occurrence'?

A. The chance that an event will happen regardless of how much damage it may cause

B. The overall impact to the organization once all factors have been considered

C. The potential for a system to have a weakness or aw that might be exploited

D. The probability that a threat actor will target and attempt to exploit an organization's systems

Answer: D

Question #:30 - (Exam Topic 1)

A technician is required to congure updates on a guest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots

B. Revert to known state

C. Rollback to known conguration

D. Shadow copy

Answer: A

Question #:31 - (Exam Topic 1)

A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning, and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR

B. FAR

C. CER

D. SLA

Answer: A

Question #:32 - (Exam Topic 1)

A company is experiencing an increasing number of systems that are locking up on Windows startup. The security analyst clones a machine, enters into safe mode, and discovers a file in the startup process that runs Wstart.bat.

```
@echo off

:asdhbawdhbasdhbawdhb

start notepad.exe

start notepad.exe

start calculator.exe

start calculator.exe

goto asdhbawdhbasdhbawdhb
```

Given the file contents and the system's issues, which of the following types of malware is present?

A. Rootkit

B. Logic bomb

C. Worm

D. Virus

Answer: B

Question #:33 - (Exam Topic 1)

A company uses WPA2-PSK, and it appears there are multiple unauthorized connected to the wireless network. A technician suspects this is because the wireless passwords has been shared with unauthorized individuals. Which of the following should the technician implement to BEST reduce the risk of this happening in the future?

A. Wireless guest isolation

B. 802.1X

C. WPS

D. MAC address blacklist

Answer: B

Question #:34 - (Exam Topic 1)

An analysis of a threat actor, which has been active for several years, reveals the threat actor has high levels of funding, motivation, and sophistication. Which of the following types of threat actors does this BEST describe?

A. Advanced persistent threat

B. Hacktivist

C. Organized crime

D. Insider

Answer: A

Question #:35 - (Exam Topic 1)

Ann a security analyst from a large organization has been instructed to use another more effective scanning tool After installing the tool on her desktop she started a full vulnerability scan After running the scan for eight hours. Ann finds that there were no vulnerabilities identified Which of the following is the MOST likely cause of not receiving any vulnerabilities on the network?

A. The organization has a zero tolerance policy against not applying cybersecurity best practices

B. The organization had a proactive approach to patch management principles and practices

C. The security analyst credentials did not allow full administrative rights for the scanning tool

D. The security analyst just recently applied operating system level patches

Answer: C

Question #:36 - (Exam Topic 1)

A network administrator was provided the following output from a vulnerability scan.

Plugin ID	Severity	Count	Description	Risk Score
10	Critical	1	CentOS 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise Which of the following plugin IDs should be remediated FIRST?

A. 10

B. 11

C. 12

D. 13

E. 14

Answer: D

Question #:37 - (Exam Topic 1)

An attacker has recently compromised an executives laptop and installed a RAT. The attacker used a registry key to ensure the RAT starts every time the laptop Is powered on. Of which of the following is this an example?

A. Pivot

B. Persistence

C. Escalation of privilege

D. Reconnaissance

Answer: B

Question #:38 - (Exam Topic 1)

Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.

B. Compare the image hash to the original hash.

C. Ensure a legal hold has been placed on the image.

D. Verify the time offset on the image file.

Answer: B

Question #:39 - (Exam Topic 1)

The web platform team is deploying a new web application During testing, the team notices the web application is unable to create a TLS connection to the API gateway. The administrator created a firewall rule that permit TLS traffic from the web application server to the API gateway. However, the firewall logs show all traffic is being dropped. Which of the following is MOST likely causing the issue'

A. The web application server and API gateway cannot negotiate a TLS cipher suite

B. The API gateway requires configuration changes to allow TLS connections from the new servers

C. The TLS connection is running over a non-standard port

D. The API gateway and web server use TLS certificate pinning

Answer: B

Question #:40 - (Exam Topic 1)

During a routine check, a security analyst discovered the script responsible for the backup of the corporate file server had been changed to the following.

```
date = get_currentdate()
if date = $userA.Birthdate then
    exec ' rm -rf /'
end if
```

Which of the following BEST describes the type of malware the analyst discovered?

A. Key logger

B. Rootkit

C. RAT

D. Logic bomb

Answer: D

Question #:41 - (Exam Topic 1)

During a network assessment a security analyst identifies that most of the egress traffic is related to port 443. The company is interested in identifying the content of this traffic, as allowed by the corporate policy. Which

of the following technologies should the security analyst deploy?

A. DLP solution

B. SSL decryptor

C. Layer 3 switch

D. Reverse proxy

E. Behavioral NIDS solution

Answer: B

Question #:42 - (Exam Topic 1)

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

A. VPN

B. Drive encryption

C. Network firewall

D. File-level encryption

E. USB blocker

F. MFA

Answer: B C

Question #:43 - (Exam Topic 1)

A law ofce has been leasing dark ber from a local telecommunications company to connect a remote ofce to company headquarters. The telecommunication company has decided to discontinue its dark ber product and is offering an MPLS connection. Which the law office feels is too expensive. Which of the following is the BEST solution for the law office?

A. Remote access VPN

B. VLAN

C. VPN concentrator

D. Site-to-site VPN

Answer: D

Question #:44 - (Exam Topic 1)

A network administrator needs 10 prevent users from accessing the accounting department records. All users are connected to the same Layer 2 device and access the internal through the same router. Which of the following should be Implemented to segment me accounting department from the rest of the users?

A. Implement VLANs and an ACL.

B. Install a firewall and create a DUZ

C. Create a site-to-site VPN.

D. Enable MAC address filtering.

Answer: D

Question #:45 - (Exam Topic 1)

A corporation with 35,000 employees replaces its staff laptops every three years. The social responsibility director would like to reduce the organization's carbon footprint and e-waste by donating the old equipment to a charity. Which of the following would be the MOST cost- and time-effective way for the corporation to prevent accidental disclosure of data and minimize additional cost to the charity?

A. Wiping

B. Formatting

C. SSD shredding

D. Degaussing

Answer: D

Question #:46 - (Exam Topic 1)

Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow

B. Zero-day

C. End of life

D. Race condition

Answer: B

Question #:47 - (Exam Topic 1)

An organization requires that all workstations he issued client computer certicates from the organization‘s PKI. Which of the following congurations should be implemented?

A. EAP-PEAP

B. LEAP

C. EAP-TLS

D. EAP-FAST/MSCHAPv2

E. EAP-MD5

Answer: C

Question #:48 - (Exam Topic 1)

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline

B. The endpoint configurations

C. The adversary behavior profiles

D. The IPS signatures

Answer: D

Question #:49 - (Exam Topic 1)

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.

B. The document is a backup file if the system needs to be recovered

C. The document is a standard file that the OS needs to verify the login credentials.

D. The document is a keylogger that stores all keystrokes should the account be compromised.

Answer: A

Question #:50 - (Exam Topic 1)

Which of the following BEST describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible

B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations

C. Implementing elliptic curve cryptographic algorithms with true random numbers

D. The use of NDAs and policy controls to prevent disclosure of company secrets

Answer: B

Question #:51 - (Exam Topic 1)

Which of the following is the BEST way to protect kiosk computers from theft in a public setting?

A. Secure the computer with a cable lock

B. Require biometric authentication

C. Use a security enclosure

D. Encrypt the hard drive

Answer: A

Question #:52 - (Exam Topic 1)

A company notices that at 10 a.m. every Thursday, three users' computers become inoperable. The security analyst team discovers a file called where.pdf.exe that runs on system startup. The contents of where.pdf.exe are shown below:

```
@echo off
if [c:\file.txt] deltree C:\
```

Based on the above information, which of the following types of malware was discovered?

A. Rootkit

B. Backdoor

C. Logic bomb

D. RAT

Answer: C

Question #:53 - (Exam Topic 1)

The phones at a business are being replaced with VoIP phones that get plugged in-line between the switch and PC The voice and data networks still need to be kept separate. Which of the following would allow for this?

A. NAT

B. Intranet

C. Subnetting

D. VLAN

Answer: D

Question #:54 - (Exam Topic 1)

The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to:

A. arbitrary code execution.

B. resource exhaustion.

C. exposure of authentication credentials.

D. dereferencing of memory pointers.

Answer: A

Question #:55 - (Exam Topic 1)

A network administrator was concerned during an audit that users were able to use the same passwords the day after a password change policy took effect. The following settings are in place:

* Users must change their passwords every 30 days.

* Users cannot reuse the last 10 passwords.

Which of the following settings would prevent users from being able to immediately reuse the same passwords?

A. Minimum password age of five days

B. Password history of ten passwords

C. Password length greater than ten characters

D. Complex passwords must be used

Answer: B

Question #:56 - (Exam Topic 1)

Staff members of an organization received an email message from the Chief Executive Officer (CEO) asking them for an urgent meeting in the main conference room. When the staff assembled, they learned the message received was not actually from the CEO. Which of the following BEST represents what happened?

A. Spear phoshing attack

B. Whaling attack

C. Phishing attack

D. Vishing attack

Answer: A

Question #:57 - (Exam Topic 1)

A technician is designing a solution that will be required to process sensitive information, including classified government data. The system needs to be common criteria certified. Which of the following should the technician select?

A. Security baseline

B. Hybrid cloud solution

C. Open-source software applications

D. Trusted operating system

Answer: D

Question #:58 - (Exam Topic 1)

A company has users and porters in multiple geographic locations and the printers are locked in common areas of the offices. To preserve the confidentially of PII, a security administrator needs to implement the appropriate controls Which of the following would BEST meet the confidentiality requirements of the data?

A. Enforcing location-based policy restrictions

B. Adding location to the standard naming convention

C. implementing time-of-day restrictions based on location

D. Conducting regular account maintenance at each location

Answer: D

Question #:59 - (Exam Topic 1)

Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. pivoting.

B. persistence.

C. active reconnaissance.

D. a backdoor.

Answer: C

Question #:60 - (Exam Topic 1)

A technician is evaluating a security appliance solution. The company needs a system that continues to pass traffic if the system crashes. Which of the following appliance feature would BEST meet the company's needs?

A. Fall closed.

B. Fall Secure

C. Fall Safe

D. Fall open

Answer: D

Question #:61 - (Exam Topic 1)

Which of the following attacks is used to capture the WPA2 handshake?

A. Replay

B. IV

C. Evil twin

D. Disassociation

Answer: A

Explanation

QUESTION 828

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate devices using PKI. Which of the following should the administrator configure?

A. A captive portal

B. PSK

C. 802.1X

D. WPS

Answer: D

Question #:62 - (Exam Topic 1)

An administrator needs to implement a connection to a supplier for confidential order processing and also provide a method for support engineers in the field to connect to the ERP. Which of the following should the administrator implement?

A. A remote access VPN for the supplier and a site-to-site VPN for the field engineers

B. A split-tunnel VPN for the supplier and a full-tunnel VPN for the field engineers

C. A VPN concentrator for the supplier and an SSL accelerator for the field engineers

D. An IPSec VPN connection for the supplier and SSL VPN connections for the field engineers

Answer: A

Question #:63 - (Exam Topic 1)

The Chief Security Officer (CSO) for an online retailer received a report from a penetration test that was performed against the company's servers. After reviewing the report, the CSO decided not to implement the recommended changes due to cost; instead, the CSO increased insurance coverage for data breaches. Which of the following describes how the CSO managed the risk?

A. Acceptance

B. Ignorance

C. Transference

D. Avoidance

Answer: C

Question #:64 - (Exam Topic 1)

Which of the following is a passive method to test whether transport encryption is implemented?

A. Black box penetration test

B. Port scan

C. Code analysis

D. Banner grabbing

Answer: B

Question #:65 - (Exam Topic 1)

A preventive control differs from a compensating control in that a preventive control is:

A. put in place to mitigate a weakness in a user control.

B. deployed to supplement an existing control that is EOL.

C. relied on to address gaps in the existing control structure.

D. designed to specifically mitigate a risk.

Answer: C

Question #:66 - (Exam Topic 1)

A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener. Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)

A. tcpdump

B. nc

C. nmap

D. nslookup

E. tail

F. tracert

Answer: B C

Question #:67 - (Exam Topic 1)

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better:

A. validate the vulnerability exists in the organization's network through penetration testing.

B. research the appropriate mitigation techniques in a vulnerability database.

C. find the software patches that are required to mitigate a vulnerability.

D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

Question #:68 - (Exam Topic 1)

Exercising various programming responses for the purpose of gaming insight into a system's security posture without exploiting the system is BEST described as.

A. passive security control testing.

B. control gap analysis

C. peer-conducted code review.

D. non-intrusive scanning

Answer: D

Question #:69 - (Exam Topic 1)

Given the information below:

MD5HASH document.doc 049eab40fd36caadlfab10b3cdf4a883

MD5HASH image.jpg 049eab40fd36caadlfab10b3cdf4a883

Which of the following concepts are described above? (Choose two.)

A. Salting

B. Collision

C. Steganography

D. Hashing

E. Key stretching

Answer: B D

Question #:70 - (Exam Topic 1)

A tester was able to leverage a pass-the-hash attack during a recent penetration test. The tester gained a foothold and moved laterally through the network Which of the following would prevent this type of attack from reoccurring?

A. Renaming all active service accounts and disabling all inactive service accounts

B. Creating separate accounts for privileged access that are not used to log on to local machines

C. Enabling full-disk encryption on all workstations that are used by administrators and disabling RDP

D. Increasing the password complexity requirements and setting account expiration dates

Answer: D

Question #:71 - (Exam Topic 1)

A company recently experienced a security breach. The security start determined that the intrusion was due to an out-of-date proprietary software program running on a non-compliant server The server was imaged and copied onto a hardened VM. with the previous connections re-established. Which of the Mowing Is the NEXT step in the incident response process?

A. Recovery

B. Eradication

C. Lessons learned

D. Containment

E. Identification

Answer: E

Question #:72 - (Exam Topic 1)

A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

Enforce password history: Three passwords remembered

Maximum password age?: 30 days

Minimum password age: Zero days

Complexity requirements: At least one special character, one uppercase

Minimum password length: Seven characters

Lockout duration: One day

Lockout threshold: Five failed attempts in 15 minutes

Which of the following adjustments would be the MOST appropriate for the service account?

A. Disable account lockouts.

B. Set the maximum password age to 15 days.

C. Set the minimum password age to seven days.

D. Increase password length lo 18 characters.

Answer: B

Question #:73 - (Exam Topic 1)

A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking equipment and media are functioning as expected, which leads the technician to QUESTION NO: certain PKI components. Which of the following should the technician use to validate this assumption? (Choose two.)

A. PEM

B. CER

C. SCEP

D. CRL

E. OCSP

F. PFX

Answer: D E

Question #:74 - (Exam Topic 1)

Which of the following is the main difference between symmetric end asymmetric cryptographic algorithms?

A. The use of PKI in symmetric algorithms

B. HSM-based key generation

C. Only one Key used in symmetric algorithms

D. Random vs pseudo-random key generation

Answer: C

Question #:75 - (Exam Topic 1)

An organization handling highly condential information needs to update its systems. Which of the following is the BEST method to prevent data compromise?

A. Wiping

B. Degaussing

C. Shredding

D. Purging

Answer: C

Question #:76 - (Exam Topic 1)

The Chief Information Officer (CIO) has heard concerns from the business and the help desk about frequent user account lockouts Which of the following account management practices should be modified to ease the burden?

A. Password complexity

B. Account disablement

C. False-rejection rate

D. Time-of-day restrictions

Answer: A

Question #:77 - (Exam Topic 1)

When conducting a penetration test, a pivot is used to describe a scenario in which:

A. the penetration tester uses pass-the-hash to gam access to a server via SMB, and then uses this server to SSH to another server

B. a penetration tester is able to download the Active Directory database after exploiting an unpatched vulnerability on the domain controller

C. the vulnerability scanner reveals a flaw in SMB signing, which can be used to send a netcat recon tool to one of the servers on the network.

D. the penetration tester is able to access the datacenter or network closet by using a lockpick

Answer: A

Question #:78 - (Exam Topic 1)

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

D18912E1457D5D1DDCBD40AB3BF70D5D

A. Key escrow

B. A self-signed certificate

C. Certificate chaining

D. An extended validation certificate

Answer: D

Question #:79 - (Exam Topic 1)

A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

* The VPN must support encryption of header and payload.

* The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel

B. Transport mode

C. Tunnel mode

D. IPSec

Answer: A

Question #:80 - (Exam Topic 1)

A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Select TWO).

A. Privileged accounts

B. Password reuse restrictions

C. Password complexity requirements

D. Password recovery

E. Account disablement

Answer: C E

Question #:81 - (Exam Topic 1)

An organization requires three separate factors for authentication to sensitive systems. Which of the following would BEST satisfy the requirement?

A. Fingerprint. PIN. and mother's maiden name

B. One-time password sent to a smartphone thumbprint. and home street address

C. Fingerprint. voice recognition, and password

D. Password, one-time password sent to a smartphone. and text message sent to a smartphone

Answer: B

Question #:82 - (Exam Topic 1)

A company recently updated its website to increase sales. The new website uses PHP forms for leads and

provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention

B. Implementing account lockouts

C. Discontinuing the use of privileged accounts

D. Increasing the minimum password length from eight to ten characters

Answer: A

Question #:83 - (Exam Topic 1)

The Chief Executive Officer (CEO) received an email from the Chief Financial Ofcer (CFO), asking the CEO to send nancial details. The CEO thought it was strange that the CFO would ask for the nancial details via email. The email address was correct in the "From “section of the email. The CEO clicked the form and sent the financial information as requested. Which of the following caused the incident?

A. Domain hijacking

B. SPF not enabled

C. MX records rerouted

D. Malicious insider

Answer: B

Question #:84 - (Exam Topic 1)

A public relations team will be taking a group of guests on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. loss of proprietary information

B. damage to the company's reputation

C. social engineering

D. credential exposure

Answer: C

Question #:85 - (Exam Topic 1)

While reviewing system logs, a security analyst notices that a large number of end users are changing their passwords four times on the day the passwords are set to expire. The analyst suspects they are cycling their passwords to circumvent current password controls. Which of the following would provide a technical control to prevent this activity from occurring?

A. Set password aging requirements.

B. Increase the password history from three to five.

C. Create an AUP that prohibits password reuse.

D. Implement password complexity requirements.

Answer: A

Question #:86 - (Exam Topic 1)

An organization has decided to host its web application and database in the cloud. Which of the following

BEST describes the security concerns for this decision?

A. Access to the organization’s servers could be exposed to other cloud-provider clients.

B. The cloud vendor is a new attack vector within the supply chain.

C. Outsourcing the code development adds risk to the cloud provider.

D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

Question #:87 - (Exam Topic 1)

A security administrator has been conducting an account permissions review that has identified several users

who belong to functional groups and groups responsible for auditing the functional groups' actions. Several recent outages have not been able to be traced to any user. Which of the following should the security administrator recommend to preserve future audit tag integrity?

A. Enforcing stricter onboarding workflow policies.

B. Applying least privilege to user group membership.

C. Following standard naming conventions for audit group users.

D. Restricting audit group membership to service accounts.

Answer: D

Question #:88 - (Exam Topic 1)

An organization's Chief Information Officer (CIO) read an article that identified leading hacker trends and attacks, one of which is the alteration of URLs to IP addresses resulting in users being redirected to malicious websites. To reduce the chance of this happening in the organization, which of the following secure protocols should be implemented?

A. DNSSEC

B. IPSec

C. LDAPS

D. HTTPS

Answer: A

Question #:89 - (Exam Topic 1)

A mobile application developer wants to secure an application that transmits sensitive information Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling

B. Chaining

C. Signing

D. Pinning

Answer: D

Question #:90 - (Exam Topic 1)

When building a hosted datacenter. Which of the following is the MOST important consideration for physical security within the datacenter?

A. Security guards

B. Cameras

C. Secure enclosures

D. Biometrics

Answer: A

Question #:91 - (Exam Topic 1)

A security analyst is performing a BIA. The analyst notes that in a disaster, failover systems must be up and running within 30 minutes. The failover systems must use backup data that is no older than one hour. Which of the following should the analyst include in the business continuity plan?

A. A maximum MTTR of 30 minutes

B. A maximum MTBF of 30 minutes

C. A maximum RTO of 60 minutes

D. A maximum RPO of 60 minutes

E. An SLA guarantee of 60 minutes

Answer: D

Question #:92 - (Exam Topic 1)

A systems administrator wants to secure a backup environment so backups are less prone to ransomware attacks. The administrator would like to have a fully isolated set of backups. Which of the following would be the MOST secure option for the administrator to Implement?

A. A DMZ

B. An air gap

C. A honeypot

D. A VLAN

Answer: B

Question #:93 - (Exam Topic 1)

While testing a new vulnerability scanner, a technician becomes concerned about reports that list security concerns that are not present on the systems being tested. Which of the following BEST describes this flaw?

A. False positives

B. Crossover error rate

C. Uncredentialed scan

D. Passive security controls

Answer: A

Question #:94 - (Exam Topic 1)

An organization has the following password policies:

• Passwords must be at least 16 characters long.

• A password cannot be the same as any previous 20 passwords.

• Three failed login attempts will lock the account for five minutes.

• Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a completely separate server. Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems; the organization should scan for password reuse across systems.

B. The organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.

C. User passwords are not sufficiently long or complex: the organization should increase the complexity and length requirements for passwords.

D. The trust relationship between the two servers has been compromised: the organization should place each server on a separate VLAN.

Answer: A

Question #:95 - (Exam Topic 1)

An administrator performs a workstation audit and finds one that has non-standard software installed. The administrator then requests a report to see if a change request was completed for the installed software. The

report shows a request was completed. Which of the following has the administrator found?

A. A baseline deviation

B. Unauthorized software

C. A license compliance violation

D. An insider threat

Answer: A

Question #:96 - (Exam Topic 1)

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operations in the event of a prolonged DDoS attack on its local datacenter that consumes server resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Upgrade the bandwidth available into the datacenter.

B. Migrate to a geographically dispersed cloud datacenter.

C. Implement a hot-site failover location.

D. Switch to a complete SaaS offering to customers.

E. Implement a challenge response test on all end-user queries.

Answer: C

Question #:97 - (Exam Topic 1)

After deploying an antivirus solution on some network-isolated industrial computers, the service desk team received a trouble ticket about the following message being displayed on then computer’s screen:

```
Your AV protection has blocked an unknown application while performing suspicious activities. The application
was put in quarantine.
```

Which of the following would be the SAFEST next step to address the issue?

A. Immediately delete the detected file from the quarantine to secure the environment and clear the alert from the antivirus console

B. Perform a manual antivirus signature update directly from the antivirus vendor's cloud

C. Centrally activate a full scan for the entire set of industrial computers, looking for new threats

D. Check the antivirus vendor's documentation about the security modules, incompatibilities, and software

whitelisting.

Answer: D

Question #:98 - (Exam Topic 1)

Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network

B. Applying a new user account with a complex password

C. Implementing a AAA framework for network access

D. Using a popular website login to provide access to another website

Answer: D

Explanation

Explanation

Question #:99 - (Exam Topic 1)

Smart home devices that ate always on or connected, such as HVAC system components, introduce SOHO networks to risks because of:

A. default factory settings and constant communication channels to cloud servers

B. strong passwords which are not known by SOHO administrators preventing security patching

C. loT devices requiring.

D. automatic firmware updates constantly shifting the threat landscape

Answer: A

Question #:100 - (Exam Topic 1)

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

* Employees must provide an alternate work location (i.e., a home address).

* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

A. Geofencing, content management, remote wipe, containerization, and storage segmentation

B. Content management, remote wipe, geolocation, context-aware authentication, and containerization

C. Application management, remote wipe, geofencing, context-aware authentication, and containerization

D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: C

Explanation

For mobile device security, you also need to consider application and content management, geofencing, geolocation, push notification services, biometrics, context-aware authentication, containerization, storage segmentation, and full device encryption.

Application management includes ensuring that only approved applications can be installed on company-owned devices.
Content management ensuring that only approved data can be stored on company-owned devices.
Remote wipe ensures that a device can be remotely wiped if lost or stolen.
Geofencing ensures that mobile devices are only functional within a certain location or geographic area.
Geolocation allows mobile devices to be located.
Push notification services alert mobile device users when operating systems or applications need to be updated.
Biometrics provide an additional authentication layer.
Context-aware authentication ensures that a mobile device is operating in a certain context to be operational.
Containerization is the practice of separating and securing a portion of a device's storage from the rest of the device. Storage segmentation is another term for containerization.
Full device encryption encrypts the entire contents of a mobile device.

Question #:101 - (Exam Topic 1)

A systems administrator wants to enforce me use of HTTPS on a new website. Which of the following should the systems administrator do NEXT after generating the CSR?

A. Install the certificate on the server

B. Provide the public key to the CA

C. Password protect the public key

D. Ensure the new key is not on the CRL

Answer: B

Question #:102 - (Exam Topic 1)

Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:

```
C:\Users\Ann\Documents\File1.pgp
C:\Users\Ann\Documents\AdvertisingReport.pgp
C:\Users\Ann\Documents\FinancialReport.pgp
```

Which of the following types of malware was executed?

A. Ransomware

B. Adware

C. Spyware

D. Virus

Answer: A

Question #:103 - (Exam Topic 1)

A security administrator is working with the human resources department to classify data held by the company. The administrator has determined the data contains a variety of data types, including health information, employee names and addresses, trade secrets, and confidential customer information. Which of the following should the security administrator do NEXT?

A. Apply a predefined set of labels from government sources to all data within the company.

B. Create a custom set of data labels to group the data by sensitivity and protection requirements.

C. Label sensitive data according to age to comply with retention policies.

D. Destroy company information that is not labeled in compliance with government regulations and laws.

Answer: B

Question #:104 - (Exam Topic 1)

Joe. a network administrator, ran a utility to perform banner grabbing to look for an older version of FTP service running on the servers. Which of the following BEST describes the underlying purpose of this approach?

A. Identify lack of security controls

B. Identify misconfigurations

C. Identify vulnerabilities

D. Identify poor firewall rules

Answer: C

Question #:105 - (Exam Topic 1)

Which of the following identity access methods creates a cookie on the rst logic to a central authority to allow logins to subsequent applications without referring credentials?

A. Multifactor authentication

B. Transitive trust

C. Federated access

D. Single sign-on

Answer: D

Question #:106 - (Exam Topic 1)

Which of the following is a component of multifactor authentication?

A. RADIUS

B. SSO

C. Transitive trust

D. OTP

Answer: A

Question #:107 - (Exam Topic 1)

A systems administrator needs to integrate multiple loT and small embedded devices into the company's wireless network securely Witch of the following should the administrator implement to ensure low-power and legacy devices can connect to the wireless network?

A. WPS

B. WPA

C. EAP-FAST

D. 802IX

Answer: A

Question #:108 - (Exam Topic 1)

Which of the following should a company require prior to performing a penetration test?

A. NDA

B. CVE score

C. Data classification

D. List of threats

Answer: B

Question #:109 - (Exam Topic 1)

A restaurant wants to deploy tablets to all waitstaff but does not want to use passwords or manage users to connect the tablets to the network. Which of the following types of authentication would be BEST suited for this scenario?

A. Proximity cards

B. IEEE 802.1x

C. Hardware token

D. Fingerprint reader

Answer: D

Question #:110 - (Exam Topic 1)

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants lo ensure il does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new dally backups that are tested on a frequent basis.

B. Restrict administrative privileges and patch all systems and applications.

C. Rebuild all workstations and Install new antivirus software.

D. Implement application whitelisting and perform user application hardening.

Answer: A

Question #:111 - (Exam Topic 1)

Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection.

B. A secret passcode that prompts the user to enter a secret key if entered correctly.

C. A digital certificate on a physical token that is unlocked with a secret passcode.

D. A one-time password token combined with a proximity badge.

Answer: D

Question #:112 - (Exam Topic 1)

Given the following output:

Which of the following BEST describes the scanned environment?

A. A host was identified as a web server that is hosting multiple domains.

B. A host was scanned, and web-based vulnerabilities were found.

C. A connection was established to a domain, and several redirect connections were identified.

D. A web shell was planted in company corn's content management system.

Answer: B

Question #:113 - (Exam Topic 1)

An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import.

B. Distribute hardware tokens to the users for authentication to the cloud.

C. Implement SAML with the organization’s server acting as the identity provider.

D. Configure a RADIUS federation between the organization and the cloud provider.

Answer: D

Question #:114 - (Exam Topic 1)

An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive.

B. Shred the hard drive.

C. Sanitize all of the data.

D. Degauss the hard drive.

Answer: B

Question #:115 - (Exam Topic 1)

A technician wants to implement PKI-based authentication on an enterprise wireless network. Which of the following should configure to enforce the use for client-site certificates?

A. 802.1X with PEAP

B. WPA2-PSK

C. EAP-TLS

D. RADIUS Federation

Answer: B

Question #:116 - (Exam Topic 1)

A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company's controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables

B. Cable locks

C. Conduits

D. Bayonet Neill-Concelman

Answer: B

Question #:117 - (Exam Topic 1)

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A split-tunnel VPN

D. Load-balanced servers

Answer: B

Explanation

By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

Question #:118 - (Exam Topic 1)

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYja16ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks Is the researcher MOST likely experiencing?

A. MAC cloning

B. Evil twin

C. Man-in-the-middle

D. ARP poisoning

Answer: C

Explanation

This is alarming because it could actually mean that you're connecting to a different server without knowing it. If this new server is malicious then it would be able to view all data sent to and from your connection, which could be used by whoever set up the server. This is called a man-in-the-middle attack. This scenario is exactly what the "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!" message is trying to warn you about.

Question #:119 - (Exam Topic 1)

Which of the following models is considered an iterative approach with frequent testing?

A. Agile

B. Waterfall

C. DevOps

D. Sandboxing

Answer: A

Question #:120 - (Exam Topic 1)

Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the windows/Currentversion/Run registry key?

A. Persistence

B. Pivoting

C. Active reconnaissance

D. Escalation of privilege

Answer: D

Question #:121 - (Exam Topic 1)

An organization's Chief Executive Officer (CEO) directs a newly hired computer technician to install an OS on the CEO‘s: personal laptop. The technician performs the installation, and a software audit later in the month indicates a violation of the EULA occurred as a result. Which of the following would address this violation going forward?

A. Security conguration baseline

B. Separation of duties

C. AUP

D. NDA

Answer: C

Question #:122 - (Exam Topic 1)

Exploitation of a system using widely known credentials and network addresses that results in DoS is an example of:

A. improper error handling.

B. default configurations.

C. untrained users

D. lack of vendor support

Answer: B

Question #:123 - (Exam Topic 1)

An organization prefers to apply account permissions to groups and not individual users, but allows for exceptions that are justified. Some systems require a machine-to-machine data exchange and an associated account to perform this data exchange. One particular system has data in a folder that must be modified by another system. No user requires access to this folder; only the other system needs access to this folder. Which of the following is the BEST account management practice?

A. Create a service account and apply the necessary permissions directly to the service account itself

B. Create a service account group, place the service account in the group, and apply the permissions on the group

C. Create a guest account and restrict the permissions to only the folder with the data.

D. Create a generic account that will only be used for accessing the folder, but disable the account until it is needed for the data exchange

E. Create a shared account that administrators can use to exchange the data but audit the shared account activity.

Answer: A

Question #:124 - (Exam Topic 1)

A chief information security officer (CISO) asks the security architect to design a method for contractors to access the company's internal wiki, corporate directory, and email services securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. vpn

B. PaaS

C. IaaS

D. VDI

Answer: A

Question #:125 - (Exam Topic 1)

Which of the following impacts MOST likely results from poor exception handling?

A. Widespread loss of confidential data

B. Network-wide resource exhaustion

C. Privilege escalation

D. Local disruption of services

Answer: A

Question #:126 - (Exam Topic 1)

A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords.

B. Use SSH for remote access.

C. Configure SNMPv2 for device management.

D. Use TFTP to copy device configuration.

Answer: B

Question #:127 - (Exam Topic 1)

Which of the following BEST describes the concept of persistence in the context of penetration testing?

A. The capability of maintaining service availability during a sustained DDoS attack providing persistent service

B. The property of a system used by penetration testers to exploit long-running network connections

C. The state where an attacker can interact with a network host's Internet-facing resources at will

D. The ability of an attacker to retain access to a system despite the best efforts to dislodge an attacker.

Answer: D

Question #:128 - (Exam Topic 1)

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap

B. Wireshark

C. Autopsy

D. DNSEnum

Answer: A

Question #:129 - (Exam Topic 1)

A Chief Information Officer (CIO) wants to eliminate the number of calls help desk is receiving for password resets when users log on to internal portals. Which of the following is the BEST solution?

A. Increase password length

B. Implement a self-service portal

C. Decrease lockout threshold

D. Deploy mandatory access control

Answer: D

Question #:130 - (Exam Topic 1)

A security analyst receives the following output

Time	Action	Host	File Name	User
12/15/2017	Policy: Endpoint USB Transfer - Blocked	Host1	Q3-Financials.PDF	User1

Which of the following MOST likely occurred to produce this output?

A. The host-based firewall prevented an attack from a Trojan horse

B. USB-OTG prevented a file from being uploaded to a mobile device

C. The host DLP prevented a file from being moved off a computer

D. The firewall prevented an incoming malware-infected file

Answer: A

Question #:131 - (Exam Topic 1)

A systems developer needs to provide machine-to-machine interface between an application and a database server in the production environment. This interface will exchange data once per day. Which of the following access control account practices would BEST be used in this situation?

A. Establish a privileged interface group and apply read-write permission to the members of that group.

B. Submit a request for account privilege escalation when the data needs to be transferred.

C. Install the application and database on the same server and add the interface to the local administrator group.

D. Use a service account and prohibit users from accessing this account for development work.

Answer: D

Question #:132 - (Exam Topic 1)

A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.

B. Open the file and run it.

C. Create a secure baseline of the system state.

D. Harden the machine.

Answer: C

Question #:133 - (Exam Topic 1)

A developer is creating a new web application on a public cloud platform and wants to ensure the application can respond to increase in load while minimizing costs during periods of low usage. Which of the following strategies is MOST relevant to the use-case?

A. Elasticity

B. Redundancy

C. High availability

D. Non-persistence

Answer: A

Question #:134 - (Exam Topic 1)

A user's laptop is being analyzed Because malware was discovered. The forensics analyst has taken the laptop off the corporate network. Following order of volatility, which of the following actions should be performed FIRST?

A. Engage the human resources department.

B. Clone me hard drive for analysis.

C. Dump the contents of the laptop's memory.

D. Inform law enforcement.

E. Take hashes of data

Answer: C

Question #:135 - (Exam Topic 1)

A Chief Security Officer (CSO) has implemented a policy to prevent the reuse of hard drives due to the risk of information spillage to unauthorized users. Which of the following would be the MOST practical process to decommission the workstations?

A. Remove all the hard drives and dispose of them in the trash.

B. Remove all the hard drives and shred the disks.

C. Remove all the hard drives and degauss them.

D. Remove all the hard drives and purge them.

Answer: B

Question #:136 - (Exam Topic 1)

A security analyst has recently deployed an MDM solution that requires biometric authentication for company-issued smartphones As the solution was implemented the help desk has seen a dramatic increase in calls by employees frustrated that company-issued phones take several attempts to unlock using the fingerprint scanner Which of the following should be reviewed to mitigate this problem?

A. Crossover error rate

B. False acceptance rate

C. False rejection rate

D. True rejection rate

Answer: A

Question #:137 - (Exam Topic 1)

A red team initiated a DoS attack on the management interface of a switch using a known vulnerability The monitoring solution then raised an alert prompting a network engineer to log in to the switch to diagnose the issue When the engineer logged in. the red team was able to capture the credentials and subsequently log in to the switch Which of the following actions should the network team take to prevent this type of breach from reoccurring?

A. Encrypt all communications with TLS 1 3

B. Transition from SNMPv2c to SNMPv3 with AES-256

C. Enable Secure Shell and disable Telnet

D. Use a password manager with complex passwords

Answer: C

Question #:138 - (Exam Topic 1)

A transitive trust:

A. is automatically established between a parent and a child.

B. is used to update DNS records.

C. allows access to untrusted domains.

D. can be used in place of a hardware token for logins.

Answer: A

Question #:139 - (Exam Topic 1)

A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?

A. Default configuration

B. Resource exhaustion

C. Memory overflow

D. Improper input handling

Answer: B

Question #:140 - (Exam Topic 1)

As part of a corporate merger. two companies are combining resources. As a result, they must transfer files through the internet in a secure manner. Which of the following protocols would BEST meet this objec1ive?(Select TWO)

A. LDAPS

B. SFTP‘

C. HTTPS

D. DNSSEC

E. SRTP

Answer: B C

Question #:141 - (Exam Topic 1)

An organization was recently compromised by an attacker who used a server certificate with the company's

domain issued by an irrefutable CA. Which of the following should be used to mitigate this risk in the future?

A. OCSP

B. DNSSEC

C. Corticated pinning

D. Key escrow

Answer: B

Question #:142 - (Exam Topic 1)

Which of the following is a security consideration for IoT devices?

A. IoT devices have built-in accounts that users rarely access.

B. IoT devices have less processing capabilities.

C. IoT devices are physically segmented from each other.

D. IoT devices have purpose-built applications.

Answer: A

Question #:143 - (Exam Topic 1)

During a penetration test, Joe, an analyst, contacts the target's service desk Impersonating a user, he attempts to obtain assistance with resetting an email password. Joe claims this needs to be done as soon as possible, as he is the vice president of sales and does not want to contact the Chief Operations Officer (COO) for approval, since the COO is on vacation. When challenged. Joe reaffirms that he needs this done immediately, and threatens to contact the service desk supervisor over the issue. Which of the following social engineering principles is Joe employing in this scenario? (Select TWO).

A. Intimidation

B. Consensus

C. Familiarity

D. Scarcity

E. Authority

Answer: C E

Question #:144 - (Exam Topic 1)

Which of the following implements a stream cipher?

A. File-level encryption

B. IKEv2 exchange

C. SFTP data transfer

D. S/MIME encryption

Answer: D

Question #:145 - (Exam Topic 1)

A security analyst has been asked to implement secure protocols to prevent cleartext credentials from being transmitted over the internal network. Which of the following protocols is the security analyst MOST likely to implement? (Select TWO).

A. SNMPv3

B. S/MIME

C. DNSSEC

D. SSH

E. SFTP

Answer: D E

Question #:146 - (Exam Topic 1)

A forensics analyst is investigating a hard drive for evidence of suspected illegal activity. Which of the following should the analyst do FIRST?

A. Create a hash of the hard drive.

B. Export the Internet history.

C. Save a copy of the case number and date as a text file in the root directory.

D. Back up the pictures directory for further inspection.

Answer: C

Question #:147 - (Exam Topic 1)

Which of the following Is a resiliency strategy that allows a system to automatically adapt to workload changes?

A. Fault tolerance

B. Redundancy

C. Elasticity

D. High availability

Answer: C

Question #:148 - (Exam Topic 1)

An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?

A. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.

B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.

C. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.

D. Use WPA2-PSK with a 24-character complex password and change the password monthly.

Answer: D

Question #:149 - (Exam Topic 1)

When accessing a popular website, a user receives a warning that the certificate for the website is not valid. Upon investigation, it was noted that the certificate is not revoked and the website is working fine for other users. Which of the following is the MOST likely cause for this?

A. The certificate Is corrupted on the server.

B. The certificate was deleted from the local cache.

C. The user needs to restart the machine.

D. The system date on the user's device is out of sync.

Answer: D

Question #:150 - (Exam Topic 1)

A security analyst is investigating a security breach involving the loss of sensitive data. A user passed the information through social media as vacation photos. Which of the following methods was used to encode the data?

A. Obfuscation

B. Steganography

C. Hashing

D. Elliptic curve

Answer: B

Question #:151 - (Exam Topic 1)

The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9. and the destination IP is 10.17.36.5. The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:

Session	Source	Destination	Protocol	Port	Action	IPS	DoS
12699	10.13.136.9	10.17.36.5	TCP	80	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	443	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	1433	DENY	YES	NO
12719	10.13.136.8	10.17.36.5	TCP	87	DENY	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	88	ALLOW	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	636	ALLOW	YES	NO
12899	10.13.126.6	10.17.36.9	UDP	9877	DENY	NO	NO

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5.

B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.

C. Request the network team to turn of IPS for 10.13.136.8 going to 10.17.36.5.

D. Request the application team to reconfigure the application and allow RPC communication.

Answer: B

Question #:152 - (Exam Topic 1)

A company help desk as received several reports that employees have experienced identify theft and compromised accounts. This occurred several days after receiving an email asking them to update their

personal bank information. Which of the following is a vulnerability that has been exploited?

A. Trojan horses

B. Phishing

C. Improperly configured accounts

D. Forged certificates

E. Untrained users

Answer: E

Question #:153 - (Exam Topic 1)

Buffer overflow can be avoided using proper.

A. memory leak prevention

B. memory reuse

C. input validation

D. implementation of ASLR

Answer: C

Question #:154 - (Exam Topic 1)

A technician is auditing network security by connecting a laptop to open hardwired jacks within the facility to verify they cannot connect. Which of the following is being tested?

A. Layer 3 routing

B. Port security

C. Secure IMAP

D. S/MIME

Answer: B

Question #:155 - (Exam Topic 1)

An organization wants to control user accounts and privileged access to database servers. The organization wants to create an audit trail of account requests and approvals, Out also wants to facilitate operational efficiency when account and access changes are needed. The organization has the following account

management practices.

• Access requests are processed through a service ticket that requires server and system owner approval.

• Once approved, user access is granted directly to the user's privileged account

• The requests and approvals are sent to the security officer where they are retained for future audits.

• Account activity and user activity are monitored and audited monthly by the business unit.

Which of the following changes should be implemented?

A. The user should be added to an existing group that already has the necessary access

B. Access requests should only be initiated by the system owner with subsequent approval by the server owner.

C. Requests and approvals should be sent to the system owner for retention

D. Account activity should be monitored dally with any violations reported to the system owner immediately.

Answer: D

Question #:156 - (Exam Topic 1)

A first responder needs to collect digital evidence from a compromised headless virtual host. Which of the following should the first responder collect FIRST?

A. Virtual memory

B. BIOS configuration

C. Snapshot

D. RAM

Answer: C

Question #:157 - (Exam Topic 1)

Joe, an employee, asks a coworker how long ago Ann started working at the help desk. The coworker expresses surprise since nobody named Ann works at the help desk. Joe mentions that Ann called several people in the customer service department 10 help reset their passwords over the phone due to unspecied “server issues.‘ Which of the following has occurred?

A. Social engineering

B. Whaling

C. Watering hots attack

D. Password cracking

Answer: A

Question #:158 - (Exam Topic 1)

An application developer is working on a new calendar and scheduling application. The developer wants to test new functionality that is time/date dependent and set the local system time to one year in the future. The application also has a feature that uses SHA-256 hashing and AES encryption for data exchange. The application attempts to connect to a separate remote server using SSL, but the connection fails. Which of the following is the MOST likely cause and next step?

A. The date is past the certificate expiration; reset the system to the current time and see if the connection still fails.

B. The remote server cannot support SHA-256; try another hashing algorithm like SHA+1 and see if the application can connect.

C. AES date/time dependent either the system time to the correct time or try a different encryption approach.

D. SSL is not the correct protocol to use in this situation-damage to TLS and by the client-server connection again

Answer: A

Question #:159 - (Exam Topic 1)

Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating

B. Corrective

C. Detective

D. Deterrent

Answer: D

Question #:160 - (Exam Topic 1)

A network administrator is implementing multifactor authentication for employees who travel and use company devices remotely by using the company VPN. Which of the following would provide the required level of authentication?

A. 802.1X and OTP

B. Fingerprint scanner and voice recognition

C. RBAC and PIN

D. Username/Password and TOTP

Answer: A

Question #:161 - (Exam Topic 1)

After a business performed a risk assessment, the current RPO has been deemed insufficient for its needs. The business decides on a new RPO. Which of the following steps should be taken NEXT?

A. The company should match its backup procedures against the new RPO.

B. The company should review its MTBF to guarantee it is tower than the new RPO

C. The company should review its MTTR to guarantee it is higher than the new RPO.

D. The company should review its access controls to guarantee the new RPO is covered

Answer: A

Question #:162 - (Exam Topic 1)

A security analyst needs a solution that can execute potential malware in a restricted and isolated environment for analysis. In which of the following technologies is the analyst interested?

A. Sandboxing

B. Staging

C. DMZ

D. Honeypot

Answer: A

Question #:163 - (Exam Topic 1)

A user from the financial aid office is having trouble interacting with the finaid directory on the university's ERP system. The systems administrator who took the call ran a command and received the following output:

```
dr-xrwx---    11  admin    common  4.OK    Feb 20      2017   .
drw-rwx-w-    31  admin    common  4.OK    Feb 20      2017   ..
-rwxr--r-x    1   admin    common  295     Jul 23      1997   .Makefile
-rwxrwxrwx    1   admin    common  69      Dec 4       2017   .makevar.mak
-rwxr-x-wx    1   admin    common  84K     Feb 25      2017   Deplpoy.carsi.Out
-rw--wxrwx    1   admin    common  295     Feb 25      1992   Makefile
drwx--x---    4   admin    admiss  4.0K    Mar 4       14:31  admissions
drwx-wx---    4   admin    common  12K     Feb 08      15:43  common
drwxrw---x    4   admin    develo  4.OK    Jan 19      16:16  development
drwx---r--    4   admin    common  12K     Feb 1       15:23  finaid
drwxr-xrw-    4   admin    hr      4.OK    Feb 27      11:59  hr
drwxrwx---    4   admin    kpi     4.OK    Mar 5       01:50  kpi
drwx---rwx    4   admin    common  4.OK    Feb 20      2017   matric
drwxrwxrw-    2   admin    common  4.OK    Sep 23      2017   obsolete
drwxrwx-w-    4   admin    studen  20K     Jan 15      16:56  student
```

Subsequently, the systems administrator has also confirmed the user is a member of the finaid group on the ERP system.

Which of the following is the MOST likely reason for the issue?

A. The permissions on the finaid directory should be drwxrwxrwx.

B. The problem is local to the user, and the user should reboot the machine.

C. The files on the finaid directory has an improper group assignment.

D. The finaid directory should be d---rwx---

Answer: A

Question #:164 - (Exam Topic 1)

A penetration tester was able to connect to a company's internal network and perform scans and staged attacks for the duration of the testing period without being noticed. The SIEM did not alert the security team to the presence of the penetration tester's devices on the network Which of the following would provide the security team with notification in a timely manner?

A. Implement rogue system detection and sensors.

B. Create a trigger on the IPS and alert the security team when unsuccessful logins occur.

C. Decrease the correlation threshold for alerts on the SIEM.

D. Run a credentialed vulnerability scan

Answer: A

Question #:165 - (Exam Topic 1)

A security analyst is reviewing the logs from a NGFWs automated correlation engine and sees the following:

Match time	Object name	Source address	Summary
2019-07-23 10:14:33	Possible Beacon Detection	10.202.10.89	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:14:52	Possible Beacon Detection	10.202.88.88	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:19:12	Potential C2 Communication Detected	10.202.55.3	Host repeatedly visited malware domains (100).
2019-07-23 10:21:21	Compromised Asset	10.202.100.12	Host is compromised based on a sequence of recent threat log activity.
2019-07-23 10:30:37	Possible Beacon Detection	10.202.123.99	Host is generating unknown TCP or UDP network traffic.
2019-07-23 10:32:03	Possible Beacon Detection	10.202.44.107	Host visited known malware URL (15).

Which of the following should the analyst perform FIRST?

A. Isolate the compromised host from the network.

B. Clear the logs and see If the same events reoccur.

C. Set up an alert to receive an email notification for all events.

D. Refresh the URL filtering database to ensure accuracy.

E. Set up a packet capture to analyze the unknown TCP and UDP traffic.

Answer: A

Question #:166 - (Exam Topic 1)

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Select Two)

A. Perform a site survey.

B. Deploy an FTK Imager.

C. Create a heat map.

D. Scan for rogue access points.

E. Upgrade the security protocols.

F. Install a captive portal

Answer: A D

Question #:167 - (Exam Topic 1)

An organization requires two separate factors as part of an authentication scheme. One of those factors is a password. Which of the following would BEST meet me requirement for the other factor?

A. Passphrase

B. OTP

C. Security question

D. PIN

Answer: B

Question #:168 - (Exam Topic 1)

While testing a new application, a developer discovers that the inclusion of an apostrophe in a username cause the application to crash. Which of the following secure coding techniques would be MOST useful to avoid this problem?

A. Input validation

B. Code signing

C. Obfuscation

D. Encryption

Answer: A

Question #:169 - (Exam Topic 1)

Given the following:

> md5.exe filel.txt

> ADIFAB103773DC6A1E6021B7E503A210

> md5.exe file2.txt

> ADIFAB103773DC6A1E602lB7E503A210

Which of the following concepts of cryptography is shown?

A. Collision

B. Salting

C. Steganography

D. Stream cipher

Answer: B

Question #:170 - (Exam Topic 1)

A startup company is using multiple SaaS and laaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM

B. DLP

C. CASB

D. SWG

Answer: C

Question #:171 - (Exam Topic 1)

Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Select TWO)

A. Unsecure protocols

B. Use of penetration-testing utilities

C. Weak passwords

D. included third-party libraries

E. Vendors/supply chain

F. Outdated anti-malware software

Answer: A C

Question #:172 - (Exam Topic 1)

An organization uses simulated phishing attacks on its users to better prepare them to recognize actual phishing attacks and get them accustomed to reporting the attacks to the security team. This is an example of:

A. baselining

B. user training

C. stress testing

D. continuous monitoring

Answer: B

Question #:173 - (Exam Topic 1)

An attacker has obtained the user ID and password of a datacenter's backup operator and has gained access to a production system. Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.

B. Initiate a confidential data exfiltration process.

C. Look for known vulnerabilities to escalate privileges.

D. Create an alternate user ID to maintain persistent access.

Answer: B

Question #:174 - (Exam Topic 1)

A company needs to implement an on-premises system that allows partner organizations to exchange order and inventory data electronically with the company over the Internet. The security architect must ensure the data is protected while minimizing the overhead associated with managing individual partner connections. Which of the following should the security architect recommend?

A. Deploy an encrypted SaaS file-sharing service

B. Set up site-to-site VPNs using ACLs

C. Develop and publish a RESTful API

D. Implement an authenticated SFTP server

Answer: B

Question #:175 - (Exam Topic 1)

A member of the IR team has identified an infected computer Which of the following IR phases should the team member conduct NEXT?

A. Eradication

B. Recovery

C. Lessons learned

D. Containment

Answer: D

Question #:176 - (Exam Topic 1)

After running an online password cracking tool, an attacker recovers the following password:

gh;jSKSTOi;618&

Based on the above information, which of the following technical controls have been implemented (Select TWO).

A. Complexity

B. Encryption

C. Hashing

D. Length

E. Salting

F. Stretching

Answer: A D

Question #:177 - (Exam Topic 1)

Which of the following is MOST likely the security impact of continuing to operate end-of-life systems?

A. Higher total cost of ownership due to support costs

B. Denial of service due to patch availability

C. Lack of vendor support for decommissioning

D. Support for legacy protocols

Answer: A

Question #:178 - (Exam Topic 1)

During the penetration testing of an organization, the tester was provided with the names of a few key servers, along with their IP address. Which of the following is the organization conducting?

A. Gray box testing

B. White box testing

C. Back box testing

D. Isolated container testing

E. Vulnerability testing

Answer: A

Question #:179 - (Exam Topic 1)

An employee on the Internet facing part of a company's website submits a 20-character phrase in a small textbox on a web form. The website returns a message back to the browser stating.

Of which of the following is this an example?

A. Resources exhaustion

B. Buffer overflow

C. Improperly configured account

D. Improper error handling

Answer: D

Question #:180 - (Exam Topic 1)

Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.

B. Users need to authenticate for each resource they access.

C. It requires an organization to configure federation.

D. The authentication is transparent to the user.

Answer: A

Question #:181 - (Exam Topic 1)

A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is an AAA solution that will provide the required wireless authentication?

A. TACACS+

B. MSCHAPv2

C. RADIUS

D. LDAP

Answer: C

Question #:182 - (Exam Topic 1)

Which of the following command line tools would be BEST to identify the services running in a server?

A. Traceroute

B. Nslookup

C. Ipconfig

D. Netstat

Answer: D

Question #:183 - (Exam Topic 1)

A network engineer needs to allow an organization's users to conned their laptops to wired and wireless networks from multiple locations and facilities, while preventing unauthorized connections to the corporate networks. Which of the following should be Implemented to fulfill the engineer's requirements?

A. Configure VLANs.

B. Install a honeypot.

C. Implement a VPN concentrator.

D. Enable MAC filtering.

Answer: C

Question #:184 - (Exam Topic 1)

Which of the following security controls BEST mitigates social engineering attacks?

A. Separation of duties

B. Least privilege

C. User awareness training

D. Mandatory vacation

Answer: C

Question #:185 - (Exam Topic 1)

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing

B. Whaling

C. Typo squatting

D. Pharming

Answer: B

Explanation

Whaling attack

A **whaling attack** is a method used by cybercriminals to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes.

A whaling attack is essentially a spear-phishing attack but the targets are bigger – hence whale phishing. Where spear-phishing attacks may target any individual, whaling attacks are more specific in what type of person they target: focusing on one specific high level executive or influencer vs a broader group of potential

victims.

Cybercriminals use whaling attacks to impersonate senior management in an organization, such as the CEO, CFO, or other executives, hoping to leverage their authority to gain access to sensitive data or money. They use the intelligence they find on the internet (and often social media) to trick employees – or another whale – into replying with financial or personal data.

Question #:186 - (Exam Topic 1)

A company has a backup site with equipment on site without any data. This is an example of:

A. a hot site.

B. a cold site.

C. a hot standby.

D. a warrn site.

Answer: D

Question #:187 - (Exam Topic 1)

A company is deploying a wireless network. It is a requirement that client devices must use X.509 certifications to mutually authenticate before connecting to the wireless network. Which of the following protocols would be required to accomplish this?

A. EAP-TTLS

B. EAP-MD5

C. LEAP

D. EAP-TLS

E. EAP-TOTP

Answer: D

Question #:188 - (Exam Topic 1)

A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

* The VPN must support encryption of header and payload.

* The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel

B. Transport mode

C. Tunnel mode

D. IPSec

Answer: A

Question #:189 - (Exam Topic 1)

Which of the following is an example of the second A in the AAA model?

A. The encryption protocol successfully completes the handshake and establishes a connection

B. The one-time password is keyed in, and the login system grants access.

C. The event log records a successful login with a type code that indicates an interactive login.

D. A domain controller confirms membership in the appropriate group

Answer: B

Question #:190 - (Exam Topic 1)

A security administration a hardening a VPN connection. Recently, company pre-shared keys were hijacked during an MITM attack and reused to breach the VPN connection. Which of the following should the security administrator do to BEST address this issue?

A. Implement PIG

B. Implement IPSec

C. Implement TLS

D. Implement PFS

Answer: A

Question #:191 - (Exam Topic 1)

Which of the following impacts MOST likely result from poor exception handling?

A. Widespread loss of condential data

B. Network-wide resource exhaustion

C. Privilege escalation

D. Local disruption of services

Answer: A

Question #:192 - (Exam Topic 1)

A coding error has been discovered on a customer-facing website. The error causes each request to return confidential PHI data for the incorrect organization. The IT department is unable to identify the specific customers who are affected. As a result, all customers must be notified of the potential breach. Which of the following would allow the team to determine the scope of future incidents?

A. Intrusion detection system

B. Database access monitoring

C. Application fuzzing

D. Monthly vulnerability scans

Answer: C

Explanation

Fuzzing is a way of finding bugs using automation. It involves providing a wide range of invalid and unexpected data into an **application** then monitoring the **application** for exceptions. The invalid data used to fuzz an **application** could be crafted for a specific purpose, or randomly generated.

Question #:193 - (Exam Topic 1)

A security administrator begins assessing a network with software that checks for available exploits against a known database using both credentials and external scripts A report will be compiled and used to confirm patching levels This is an example of

A. penetration testing

B. fuzzing

C. static code analysis

D. vulnerability scanning

Answer: D

Question #:194 - (Exam Topic 1)

A security administrator is choosing an algorithm to generate password hashes. Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5

B. 3DES

C. AES

D. SHA-1

Answer: D

Question #:195 - (Exam Topic 1)

A developer is building a new web portal for internal use. The web portal will only the accessed by internal users and will store operational documents. Which of the following certicate types should the developer install if the company is MOST interested in minimizing costs?

A. Wildcard

B. Code signing

C. Root

D. Self-signed

Answer: A

Question #:196 - (Exam Topic 1)

A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0C-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding

B. URL redirection

C. ARP poisoning

D. DNS hijacking

Answer: C

Explanation

ARP Poisoning (also known as **ARP Spoofing**) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious **ARP** packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. **ARP** Protocol translates IP addresses into MAC addresses.

Question #:197 - (Exam Topic 1)

Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain

B. Notoriety

C. Political expression

D. Corporate espionage

Answer: B

Question #:198 - (Exam Topic 1)

An information systems owner has decided to create a more stringent password policy based on recent reports that systems are being compromised with current user credentials. The current policy has password complexity reuse and history measures in place, however, attackers are repeatedly gaming access to the systems after passwords have been changed. Which of the following would be the BEST method to add to the password policy to prevent compromise?

A. Password recovery

B. Account expiration

C. Password length

D. Account lockout

Answer: B

Question #:199 - (Exam Topic 1)

Poor inventory control practices can lead to undetected and potentially catastrophic system exploitation due to:

A. diversion of capital funds to cover leased equipment costs.

B. license exhaustion as a result of protecting more devices.

C. control gaps resulting from unmanaged hosts.

D. missing SIEM threat feed updates.

Answer: C

Question #:200 - (Exam Topic 1)

A user attempts to send an email to an external domain and quickly receives a bounce-back message. The user then contacts the help desk stating the message is important and needs to be delivered immediately. While digging through the email logs, a systems administrator finds the email and bounce-back details:

Your email has been rejected because It appears to contain SSN Information. Sending SSN information via email external recipients violates company policy.

Which of the following technologies successfully stopped the email from being sent?

A. DLP

B. UTM

C. WAF

D. DEP

Answer: D

Question #:201 - (Exam Topic 1)

An organization uses multifactor authentication to restrict local network access. It requires a PIV and a PIN. Which of the following factors is the organization using?

A. Something you have; something you are

B. Something you know, something you do

C. Something you do, something you are

D. Something you have, something you know

Answer: D

Question #:202 - (Exam Topic 1)

A Security analyst has received an alert about PII being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

A. S/MIME

B. DLP

C. IMAP

D. HIDS

Answer: D

Explanation

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

Question #:203 - (Exam Topic 1)

Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption

B. Blockchain

C. Transport Layer Security

D. Perfect forward secrecy

Answer: D

Question #:204 - (Exam Topic 1)

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon Investigation, a security analyst identifies the following:

* The legitimate website's IP address is 10.1.1.20 and eRecruit.local resolves to this IP.

* The forged website's IP address appears to be 10.2.12.99. based on NetFlow records.

* All three of the organization's DNS servers show the website correctly resolves to the legitimate IP.

* DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

A. A reverse proxy was used to redirect network traffic.

B. An SSL strip MITM attack was performed.

C. An attacker temporarily poisoned a name server.

D. An ARP poisoning attack was successfully executed.

Answer: B

Question #:205 - (Exam Topic 1)

A security analyst wants to limit the use of USB and external drives to protect against malware. as well as protect les leaving a user's computer. Which of the following is the BEST method to use?

A. Firewall

B. Router

C. Antivirus software

D. Data loss prevention

Answer: D

Question #:206 - (Exam Topic 1)

Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.

B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases.

C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often

D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII

Answer: B

Question #:207 - (Exam Topic 1)

Which of the following is a symmetric encryption that applies the encryption over multiple iterations?

A. RC4

B. RSA

C. 3DES

D. SHA

Answer: B

Question #:208 - (Exam Topic 1)

A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the Internet and terminating on the company's secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers' CA full certificate chain must be installed on the UTM.

B. The UTM certificate pair must be installed on the web servers.

C. The web servers' private certificate must be installed on the UTM.

D. The UTM and web servers must use the same certificate authority.

Answer: A

Question #:209 - (Exam Topic 1)

A network administrator is trying to provide the most resilient hard drive configuration in a server. With five hard drives, which of the following is the MOST fault-tolerant configuration?

A. RAID 1

B. RAID 5

C. RAID 6

D. RAID 10

Answer: B

Question #:210 - (Exam Topic 1)

A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate.

B. Install the intermediate certificate.

C. Generate a CSR.

D. Encrypt the private key.

Answer: C

Question #:211 - (Exam Topic 1)

A critical web application experiences slow response times during the end of a company's fiscal year. This web application typically sees a 35% increase in utilization during this time. The Chief Information Officer (CIO) wants an automated solution in place to deal with the annual spike. Which of the following does the CIO MOST likely want to implement?

A. Scalability

B. Elasticity

C. Redundancy

D. High availability

Answer: B

Question #:212 - (Exam Topic 1)

An organization discovers that unauthorized applications have been installed on company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following Is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected Willi malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.

B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.

C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.

D. Some advanced users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

Answer: B

Question #:213 - (Exam Topic 1)

Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack

B. Credential harvesting

C. Hybrid warfare

D. Pharming

Answer: A

Question #:214 - (Exam Topic 1)

After discovering a buffer overflow vulnerability an application the security analyst needs to report it to the development team leader. Which of the following are MOST to appear m the impact section of the report? (Select TWO).

A. An attacker can obtain privileged data handled by the application

B. An attacker can inject DLLs into the server via the application

C. An attacker can pivot to other servers using the application

D. An attacker can execute arbitrary code using the application

E. An attacker can execute a DDoS on the server

Answer: D E

Question #:215 - (Exam Topic 1)

A company's IT staff is given the task of securely disposing of 100 server HDDs. The security team informs the IT staff that the data must not be accessible by a third party after disposal. Which of the following is the MOST time-efficient method to achieve this goal?

A. Use a degausser to sanitize the drives.

B. Remove the platters from the HDDs and shred them.

C. Perform a quick format of the HDD drives.

D. Use software to zero fill all of the hard drives.

Answer: A

Question #:216 - (Exam Topic 1)

A network administrator was recently terminated. A few weeks later, the new administrator noticed unauthorized changes to several devices that are causing denial of services. Additionally, the administrator noticed an unusual connection from an external IP address to an internal server. Which of the following is the MOST likely cause of the problem?

A. Spyware

B. Virus

C. Ransomware

D. Backdoor

Answer: D

Question #:217 - (Exam Topic 1)

An email systems administrator is configuring the mail server to prevent spear phishing attacks through email messages. Which of the following refers to what the administrator is doing?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

Answer: B

Question #:218 - (Exam Topic 1)

A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS

B. DoS

C. Zero day

D. Logic bomb

Answer: A

Question #:219 - (Exam Topic 1)

An organization has created a review process to determine how to best handle data with different sensitivity levels. The process includes the following requirements:

• Soft copy Pll must be encrypted.

• Hard copy Pll must be placed In a locked container.

• Soft copy PHI must be encrypted and audited monthly.

• Hard copy PHI must be placed in a locked container and inventoried monthly.

Locked containers must be approved and designated for document storage. Any violations must be reported to the Chief Security Officer {CSO}.

While searching for coffee in the kitchen, an employee unlocks a cabinet and discovers a list of customer names and phone numbers. Which of the following actions should the employee take?

A. Put the document back in the cabinet, lock the cabinet, and report the incident to the CSO.

B. Take custody of the document, secure it at a desk, and report the incident to the CSO.

C. Take custody of the document and immediately report the incident to the CSO.

D. Put the document back in the cabinet, inventory the contents, lock the cabinet, and report the incident to the CSO.

Answer: A

Question #:220 - (Exam Topic 1)

A technician suspects that a desktop was compromised with a rootkit. After removing lhe hard drive from the desktop and running an offline le integrity check, the technician reviews the following output:

File name	Expected hash	Installed hash	Available version	Installed version
notepad.exe	48D403AD1FAB103BD04732ACB4B3A922	48D403AD1FAB103BD04732ACB4B3A922	49.33.21	48.100.2
kernel.dll	AB502DE1A78AD1FAB1010AB3AFD45021	1AC406DE49564AD1FAB1019DDA264120	1.01.200	1.01.200
lsass.exe	0987352AB3823AAD1FAB1083AB94D3EE	0987352AB3823AAD1FAB1083AB94D3EE	0.900.20	0.900.12
httpd.exe	AD1FAB10492839FAB109283AA38549AA	AD1FAB10492839FAB109283AA38549AA	10.200.1	10.200.0

Based on the above output, which of the following is the malicious file?

A. notepad.exe

B. lsass.exe

C. kernel.dll

D. httpd.axe

Answer: C

Question #:221 - (Exam Topic 1)

A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM. Which of the following is the administrator protecting against?

A. VM sprawl

B. VM escape

C. VM migration

D. VM sandboxing

Answer: B

Question #:222 - (Exam Topic 1)

After a breach, a company has decided to implement a solution to better understand the technique used by the attackers. Which of the following is the BEST solution to be deployed?

A. Network analyzer

B. Protocol analyzer

C. Honeypot network

D. Configuration compliance scanner

Answer: C

Question #:223 - (Exam Topic 1)

An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the

engineer's requirements?

A. NIPS

B. HIDS

C. Web proxy

D. Elastic load balancer

E. NAC

Answer: A

Question #:224 - (Exam Topic 1)

A security analyst recommends implementing SSL for an existing web service. A technician installs the SSL certificate and successfully tests the connection on the server Soon after, the help desk begins receiving calls from users who are unable to log in After further investigation, it becomes clear that no users have successfully logged in since the certificate installation. Which of the following is MOST likely the issue?

A. Incorrect firewall rules are blocking HTTPS traffic.

B. Users are still accessing the IP address and not the HTTPS address.

C. Workstations need an updated trusted sites list

D. Users are not using tokens to log on.

Answer: B

Question #:225 - (Exam Topic 1)

A security team has downloaded a public database of the largest collection of password dumps on the Internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list. Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity

B. Password complexity, least privilege, password reuse

C. Password reuse, password complexity, password expiration

D. Group policy, password history, password encryption

Answer: A

Question #:226 - (Exam Topic 1)

Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment, then to systems in a staging environment, and finally to production systems.

B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems

C. Test the patches in a test environment, apply them to the production systems, and then apply them to a staging environment.

D. Apply the patches to the production systems, apply them in a staging environment, and then test all of them in a testing environment.

Answer: D

Question #:227 - (Exam Topic 1)

After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server

B. NTLM service

C. LDAP service

D. NTP server

Answer: D

Question #:228 - (Exam Topic 1)

A security team has completed the installation of a new server. The OS and applications have been patched and tested, and the server is ready to be deployed. Which of the following actions should be taken before deploying the new server?

A. Disable the default accounts.

B. Run a penetration test on the network.

C. Create a DMZ In which to place the server.

D. validate the integrity of the patches.

Answer: A

Question #:229 - (Exam Topic 1)

A security administrator has created a new group policy object that utilizes the trusted platform module to compute a hash of system files and compare the value to a known-good value. Which of the following security concepts is this an example of?

A. Integrity measurement

B. Secure baseline

C. Sandboxing

D. Immutable systems

Answer: A

Question #:230 - (Exam Topic 1)

Which of the following can be used to increase the time needed to brute force a hashed password?

A. BCRYPT

B. ECDHE

C. Elliptic curve

D. Diffie-Hellman

Answer: C

Question #:231 - (Exam Topic 1)

An organization has hired a security analyst to perform a penetration test. The analyst captures 1GB worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to future review the pcap?

A. Nmap

B. cURL

C. Netcat

D. Wireshark

Answer: D

Question #:232 - (Exam Topic 1)

Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible

B. To allow access to web services of internal users of the organization

C. To maintain connection status of all HTTP requests

D. To deny access to all websites with certain contents

Answer: A

Question #:233 - (Exam Topic 1)

A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identify redundant and high-availability systems.

B. Identity mission-critical applications and systems.

C. Identify the single point of failure in the system.

D. Identity the impact on safety of the property.

Answer: B

Question #:234 - (Exam Topic 1)

An organization is concerned about video emissions from users' desktops. Which of the following is the BEST solution to implement?

A. Screen filters

B. Shielded cables

C. Spectrum analyzers

D. Infrared detection

Answer: A

Question #:235 - (Exam Topic 1)

After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach. Which of the following steps in the incident response process has the administrator just completed?

A. Containment

B. Eradication

C. Recovery

D. Identification

Answer: B

Question #:236 - (Exam Topic 1)

The Chief Information Security Officer (CISO) at a large company tasks a security administrator to provide additional validation for website customers. Which of the following should the security administrator implement?

A. HTTP

B. DNSSEC

C. 802.1X

D. Captive portal

Answer: D

Question #:237 - (Exam Topic 1)

A technician is required to configure updates on a guest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots

B. Revert to known state

C. Rollback to known configuration

D. Shadow copy

Answer: A

Question #:238 - (Exam Topic 1)

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types Is an IDS?

A. Corrective

B. Physical

C. Detective

D. Administrative

Answer: C

Question #:239 - (Exam Topic 1)

Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap

B. Secure cabinet

C. Faraday cage

D. Safe

Answer: C

Question #:240 - (Exam Topic 1)

In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference

B. Avoidance

C. Acceptance

D. Mitigation

Answer: B

Question #:241 - (Exam Topic 1)

Which of the following implements a lossy algorithm?

A. Blowfish

B. ROT13

C. Diffie-Hellman

D. SHA

Answer: D

Question #:242 - (Exam Topic 1)

An administrator is setting up automated remote file transfers to another organization. The other organization has the following requirements for the connection protocol.

• Encryption in transit is required

• Mutual authentication must be used.

• Certificate authentication must be used {no passwords).

Which of the following should the administrator choose?

A. SNMPv3

B. SFTP

C. TLS

D. LDAPS

E. SRTP

Answer: B

Question #:243 - (Exam Topic 1)

A company is performing an analysis of the corporate enterprise network with the intent of identifying any one system, person, function, or service that, when neutralized, will cause or cascade disproportionate damage to the company's revenue, referrals, and reputation. Which of the following is an element of the BIA that this action is addressing?

A. Identication of critical systems

B. Single point of failure

C. Value assessment

D. Risk register

Answer: D

Explanation

QUESTIO NO: 22

Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak

B. SQL injection

C. Resource exhaustion

D. Buffer overow

Answer: D

QUESTIO NO: 23

A security administrator is creating a risk assessment on BYOD. One of the requirements of the risk assessment is to address the following

•Centrally managing mobile devices

•Data loss prevention

Which of the following recommendations should the administrator include in the assessment? (Select TWO).

A. implement encryption.

B. implement hashing.

C. implement an MDM with mobile device hardening.

D. implement a VPN with secure connection in webmail.

E. implement and allow cloud storage features on the network.

Answer: C, E

QUESTIO NO: 24

Condential corporate data was recently stolen by an attacker who exploited data transport protections. Which of the following vulnerabilities is the MOST likely cause of this data breach?

A. Resource exhaustion on the VPN concentrators

B. Weak SSL cipher strength

C. Improper input handling on the FTP site

D. Race condition on the packet inspection rewall

Answer: C

QUESTIO NO: 25

A user wants to send a condential message to a customer to ensure unauthorized users cannot access the information. Which of the following can be used to ensure the security of the document while in transit and at rest?

A. BCRYPT

B. PGP

C. FTPS

D. S/MIME

Answer: B

Question #:244 - (Exam Topic 1)

Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements

B. Secure configuration guide

C. Application installation guides

D. User manuals

Answer: B

Question #:245 - (Exam Topic 1)

An administrator is setting up automated remote file transfers to another organization. The other organization has the following requirements for the connection protocol:

• Encryption in transit is required.

• Mutual authentication must be used.

• Certificate authentication must be used (no passwords).

Which of the following should the administrator choose?

A. SNMPv3

B. SFTP

C. TLS

D. LDAPS

E. SRTP

Answer: B

Question #:246 - (Exam Topic 1)

Management wants to ensure any sensitive data on company-provided cell phones is isolated in a single location that can be remotely wiped if the phone is lost. Which of the following technologies BEST meets this need?

A. Geofencing

B. Containerization

C. Device encryption

D. Sandboxing

Answer: D

Question #:247 - (Exam Topic 1)

If a current private key is compromised, which of the following would ensure it cannot be used to decrypt all historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

Answer: D

Question #:248 - (Exam Topic 1)

After successfully breaking into several networks and infecting multiple machines with malware. hackers contact the network owners, demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers

B. Organized crime

C. Insiders

D. Hacktivists

Answer: B

Explanation

A person who gains unauthorized access to computer files or networks in order to further social or political ends.

Question #:249 - (Exam Topic 1)

An Organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.

The application team receive a report with the following results:

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate If the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?

A. Remediate 2633 and 3124 immediately.

B. Process a risk acceptance for 2633 and 3124.

C. Process a risk acceptance for 2633 and remediate 3124.

D. Shut down NYAccountingProd and Investigate the reason for the different scan results.

Answer: C

Question #:250 - (Exam Topic 1)

A security analyst is implementing mobile device security for a company. To save money, management has

decided on a BYOD model. The company is most concerned with ensuring company data will not be exposed if a phone is lost or stolen. Which of the following techniques BEST accomplish this goal (Select TWO).

A. Containerization

B. Full device encryption

C. Geofencing

D. Remote wipe

E. Application management

F. Storage segmentation

Answer: A B

Question #:251 - (Exam Topic 1)

A systems engineer wants to leverage a cloud-based architecture with low latency between network-connected devices that also reduces the bandwidth that is required by performing analytics directly on the endpoints. Which of the following would BEST meet the requirements? (Select TWO).

A. Private cloud

B. SaaS

C. Hybrid cloud

D. laaS

E. DRaaS

F. Fog computing

Answer: C F

Question #:252 - (Exam Topic 1)

A security analyst is investigating a call from a user regarding one of the websites receiving a 503: Service Unavailable error. The analyst runs a netstat -an command to discover if the web server is up and listening. The analyst receives the following output:

TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT

TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT

TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT

TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT

TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT

TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT

Which of the following types of attack is the analyst seeing?

A. Buffer overflow

B. Domain hijacking

C. Denial of service

D. ARP poisoning

Answer: C

Question #:253 - (Exam Topic 1)

When choosing a hashing algorithm for storing passwords in a web server database, which of the following is the BEST explanation for choosing HMAC-MD5 over simple MD5?

A. HMAC provides hardware acceleration thus speeding up authentication

B. HMAC adds a transport layer handshake which improves authentication

C. HMAC-MD5 can be decrypted taster speeding up performance

D. HMAC-M05 is more resistant to brute forcing

Answer: A

Question #:254 - (Exam Topic 1)

The director of information security at a company has recently directed the security engineering team to implement new security technologies aimed at reducing the impact of insider threats. Which of the following tools has the team MOST likely deployed? (Select TWO).

A. DLF

B. UTM

C. SFTP

D. SSH

E. SSL

Answer: A B

Question #:255 - (Exam Topic 1)

Several systems and network administrators are determining how to manage access to a facility and enable managers to allow after-hours access. Which of the following access control methods should managers use to assign after-hours access to the employees?

A. Rule-based access control

B. Discretionary access control

C. Mandatory access control

D. Role-based access control

Answer: A

Question #:256 - (Exam Topic 1)

After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ

B. A VPN

C. C. A VLAN

D. An ACL

Answer: C

Question #:257 - (Exam Topic 1)

Which of the following physical security controls is MOST effective when trying to prevent tailgating?

A. CCTV

B. Mantrap

C. Biometrics

D. RFID badge

E. Motion detection

Answer: B

Question #:258 - (Exam Topic 1)

A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at the same time. Which of the following is the BEST control to address this audit finding?

A. Faraday cage

B. Mantrap

C. Biometrics

D. Proximity cards

Answer: B

Question #:259 - (Exam Topic 1)

A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the net-work and begin authenticating users again?

A. Preparation

B. Identification

C. Containment

D. Eradication

E. Recovery

F. Lessons learned

Answer: E

Question #:260 - (Exam Topic 1)

A critical enterprise component whose loss or destruction would significantly impede business operations or have an outsized impact on corporate revenue is known as:

A. a single point of failure

B. critical system infrastructure

C. proprietary information.

D. a mission-essential function

Answer: D

Question #:261 - (Exam Topic 1)

The CSIRT is reviewing the lessons learned from a recent incident A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.

B. Segment the network with firewalls

C. Update all antivirus signatures daily

D. Implement application blacklisting.

Answer: C

Question #:262 - (Exam Topic 1)

A security analyst received an after-hours alert indicating that a large number of accounts with the suffix "admin'' were locked out. The accounts were all locked out after five unsuccessful login attempts, and no other accounts on the network triggered the same alert. Which of the following is the BEST explanation for these alerts?

A. The standard naming convention makes administrator accounts easy to identify, and they were targeted for an attack.

B. The administrator accounts do not have rigid password complexity rules, and this made them easier to crack.

C. The company has implemented time-of-day restrictions, and this triggered a false positive alert when the administrators tried to log in.

D. The threshold for locking out administrator accounts is too high, and it should be changed from five to three to prevent unauthorized access attempts.

Answer: A

Question #:263 - (Exam Topic 1)

An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk

B. Processor cache

C. Processes in running memory

D. Swap space

Answer: A

Question #:264 - (Exam Topic 1)

A security analyst is reviewing the following log:

TIME	INTERNALHOST	EXTERNAL HOST	INFORMATION
2019-07-14 14:22:01	192.168.214.10:9001	46.34.195.67:22	SYN SENT
2019-07-14 14:22:01	192.168.214.10:9001	46.34.195.67:25	SYN SENT
2019-07-14 14:22:01	192.168.214.10:9001	46.34.195.67:80	SYN SENT
2019-07-14 14:22:02	192.168.214.10:9001	46.34.195.67:443	SYN SENT
2019-07-14 14:22:02	192.168.214.10:9001	46.34.195.67:3389	SYN SENT
2019-07-14 14:22:03	192.168.214.10:9001	46.34.195.67:8080	SYN SENT

Which of the following should the analyst report to the security manager?

A. A host is attempting to enumerate the firewall ACL using an Xmas scan

B. Host 192-168.214.10 is performing a scan of well-known ports

C. An external host is scanning an internal host for vulnerable services

D. An external host is attempting to perform NAT traversal

Answer: C

Question #:265 - (Exam Topic 1)

In the event of a security incident, which of the following should be captured FIRST?

A. An external hard drive

B. System memory

C. An internal hard drive

D. Network interface data

Answer: B

Question #:266 - (Exam Topic 1)

Ann. a user, reports she is receiving emails that appear to be from organizations to which she belong. Put me emails contain links to websites that do not belong to those organizations. Which of the following security scenarios does this describe?

A. A hacker is using Ann's social media information to create a spear phishing attack.

B. The DNS servers for the organizations have been hacked and are pointing to malicious sites.

C. The company's maw system has changed the organization's links to point to a proxy server for security.

D. Ann's computer is infected with adware that has changed me email links

Answer: A

Question #:267 - (Exam Topic 1)

A healthcare company is revamping its IT strategy in light of recent regulations. The company is concerned about compliance and wants to use a pay-per-use model. Which of the following is the BEST solution?

A. On-premises hosting

B. Community cloud

C. Hosted infrastructure

D. Public SaaS

Answer: D

Question #:268 - (Exam Topic 1)

A credentialed vulnerability scan is often preferred over a non-credentialed scan because credentialed scans:

A. generates more false positives.

B. rely solely on passive measures.

C. are always non-intrusive.

D. provide more accurate data.

Answer: D

Question #:269 - (Exam Topic 1)

Which of the following is MOST likely caused by improper input handling?

A. Loss of database tables

B. Untrusted certificate warning

C. Power off reboot loop

D. Breach of firewall ACLs

Answer: A

Question #:270 - (Exam Topic 1)

A NIPS administrator needs to install a new signature to observe the behavior of a worm that may be spreading over SMB Which of the following signatures should be installed on the NIPS'?

A. PERMIT from ANY:ANY to ANY:445 regex '.-SMB.-'

B. DROP from ANY:445 Co ANY:445 regex '.-SMB.*'

C. DENY from ANY:ANY Co ANY:445 regex '.*SMB.*'

D. RESET from ANY:ANY co ANY:445 regex '.-3MB.-'

Answer: D

Question #:271 - (Exam Topic 1)

A company is looking for an all-in-one solution to provide identification authentication, authorization, and accounting services. Which of the following technologies should the company use?

A. Diameter

B. SAML

C. Kerberos

D. CHAP

Answer: D

Question #:272 - (Exam Topic 1)

The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: *File format not recognized*. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware

B. Polymorphic virus

C. Rootkit

D. Spyware

Answer: A

Question #:273 - (Exam Topic 1)

Which of the following has the potential to create a DoS attack on a system?

A. A server room WiFi thermostat with default credentials

B. A surveillance camera that has been replaced and is not plugged in

C. A disabled user account that has not been deleted

D. A wireless access point with WPA2 connected to the network

Answer: D

Question #:274 - (Exam Topic 1)

An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. DNS hijacking

B. Cross-site scripting

C. Domain hijacking

D. Man-in-the-browser

E. Session hijacking

Answer: A E

Question #:275 - (Exam Topic 1)

A company uses WPA2-PSK. and it appears there are multiple unauthorized devices connected to the wireless network A technician suspects this is because the wireless password has been shared with unauthorized individuals. Which of the following should the technician implement to BEST reduce the risk of this happening in the future?

A. Wireless guest isolation

B. 802.1X

C. WPS

D. MAC address blacklist

Answer: C

Question #:276 - (Exam Topic 1)

A security administrator is implementing a SIEM and needs to ensure events can be compared against each other based on when the events occurred and were collected. Which of the following does the administrator need to implement to ensure this can be accomplished?

A. TOTP

B. TKJP

C. NTP

D. HOTP

Answer: C

Question #:277 - (Exam Topic 1)

A company is examining possible locations for a hot site. Which of the following considerations is of MOST concern if the replication technology being used is highly sensitive to network latency?

A. Connection to multiple power substations

B. Location proximity to the production site

C. Ability to create separate caged space

D. Positioning of the site across international borders

Answer: B

Question #:278 - (Exam Topic 1)

A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed

B. Passive

C. Port

D. Credentialed

E. Red team

F. Active

Answer: D

Question #:279 - (Exam Topic 1)

An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures

B. Permission auditing

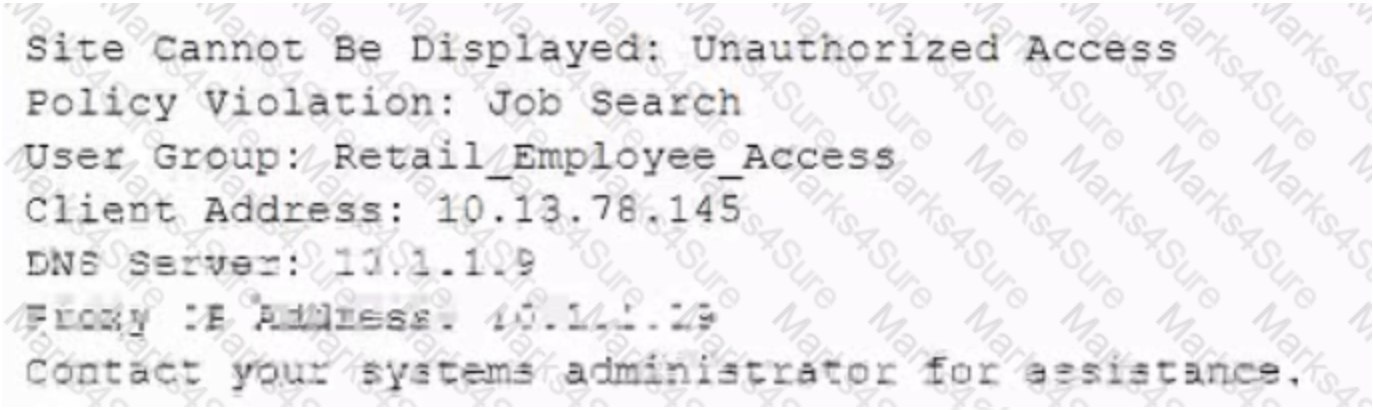
C. Roles and responsibilities

D. Communication methodologies

Answer: C

Question #:280 - (Exam Topic 1)

A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:



Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer.

B. Add the employee to a less restrictive group on the content filter.

C. Remove the proxy settings from the employee's web browser.

D. Create an exception for the job search sites in the host-based firewall on the employee's computer.

Answer: B

Question #:281 - (Exam Topic 1)

An authorized user is conducting a penetration scan of a system for an organization. The tester has a set of network diagrams. Source code, version numbers of applications. and other information about the system. Including hostnames and network addresses. Which of the following BEST describes this type of penetration test?

A. Gray-box testing

B. Black-boxtestlng

C. White-box testing

D. Blue team exercise

E. Red team exercise

Answer: C

Question #:282 - (Exam Topic 1)

Joe a new employee, discovered a thumb drive with the company's logo on it while walking in the parking lot Joe was curious as to the contents of the drive and placed it into his work computer. Shortly after accessing the contents, he noticed the machine was running slower, started to reboot, and displayed new icons on the screen.

Which of the following types of attacks occurred?

A. Social engineering

B. Brute force attack

C. MITM

D. DoS

Answer: A

Question #:283 - (Exam Topic 1)

A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public

B. Community

C. Private

D. Hybrid

Answer: B

Question #:284 - (Exam Topic 1)

A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical server must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA. Which of the following will the engineer MOST likely use to achieve this objective?

A. A forward proxy

B. A stateful firewall

C. A jump server

D. A port tap

Answer: B

Question #:285 - (Exam Topic 1)

A technician wants to configure a wireless router at a small office that manages a family-owned dry cleaning business. The router will support five laptops, potential smartphones, a wireless printer, and occasional guests.

Which of the following wireless configuration is BEST implemented in this scenario?

A. Single SSID with WPA2-Enterprise

B. 802.1X with guest VLAN

C. Dual SSID with WPA2-PSK

D. Captive portal with two-factor authentication

Answer: B

Question #:286 - (Exam Topic 1)

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.

B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.

C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox.

D. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

Answer: D

Question #:287 - (Exam Topic 1)

To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS

B. SPF

C. DMARC

D. DNSSEC

Answer: D

Question #:288 - (Exam Topic 1)

A malicious actor compromises a legitimate website, configuring it to deliver malware to visitors of the website. Which of the following attacks does this describe?

A. Whaling

B. Watering hole

C. Impersonation

D. Spoofing

Answer: A

Question #:289 - (Exam Topic 1)

A systems engineer is setting up a RADIUS server to support a wireless network that uses certificate authentication. Which of the following protocols must be supported by both the RADIUS server and the WAPs?

A. CCMP

B. TKIP

C. WPS

D. EAP

Answer: D

Question #:290 - (Exam Topic 1)

A new PKI is being bum at a company, but the network administrator has concerns about spikes of traffic occurring twice a flay due to clients checking the status of the certificates. Which of the following should be implemented to reduce the spikes in traffic?

A. CRL

B. OCSP

C. SAN

D. OID

Answer: A

Question #:291 - (Exam Topic 1)

Which of the following types of security testing is the MOST cost-effective approach used to analyze existing code and identity areas that require patching?

A. Black box

B. Gray box

C. White box

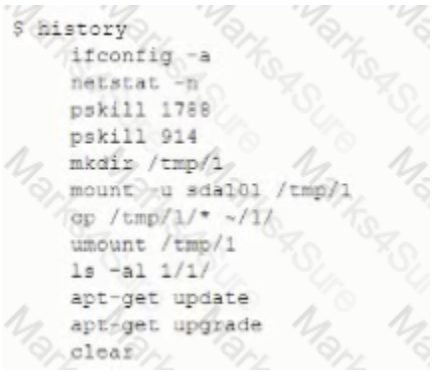
D. Red team

E. Blue team

Answer: C

Question #:292 - (Exam Topic 1)

A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:



Given this output, which of the following security issues has been discovered?

A. A misconfigured HlDS

B. A malware Installation

C. A policy violation

D. The activation of a Trojan

Answer: C

Question #:293 - (Exam Topic 1)

An organization has the following password policies:

• Passwords must be at least 16 characters long.

• Three tailed login attempts will lock the account (or live minutes.

• Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on the same server. Which of the following is MOST likely the issue, and what should be done?

A. Some users have reset their account to a previously used password; implement a password history policy.

B. Service accounts are being used to log onto the server; restrict service account permissions to read/ write.

C. Single sign-on is allowing remote logins to the database server; disable single sign-on until it can be properly configured.

D. Users are logging in after working hours; implement a time-of-day restriction for the database servers.

Answer: D

Question #:294 - (Exam Topic 1)

A corporation wants to allow users who work for its affiliate companies to sign on to each other's wireless network with their own company's credentials. Which of the following architectures would support this requirement?

A. Open authentication

B. Key escrow

C. RADIUS federation

D. Certificate chaining

Answer: A

Question #:295 - (Exam Topic 1)

Which of the following BEST distinguishes Agile development from other methodologies in terms of vulnerability management?

A. Cross-functional teams

B. Rapid deployments

C. Daily standups

D. Peer review

E. Creating user stories

Answer: C

Question #:296 - (Exam Topic 1)

While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep.

B. Physically check each system.

C. Deny Internet access to the "UNKNOWN" hostname.

D. Apply MAC filtering.

Answer: A

Question #:297 - (Exam Topic 1)

During certain vulnerability scanning scenarios, It is possible for the target system to react in unexpected ways. This type of scenario is MOST commonly known as:

A. intrusive testing.

B. a butter overflow.

C. a race condition

D. active reconnaissance.

Answer: D

Question #:298 - (Exam Topic 1)

A Chief Information Security Officer (CISO) for a school district wants to enable SSL to protect all of the public-facing servers in the domain. Which of the following is a secure solution that is the MOST cost effective?

A. Create and install a self-signed certificate on each of the servers in the domain.

B. Purchase a load balancer and install a single certificate on the load balancer.

C. Purchase a wildcard certificate and implement it on every server.

D. Purchase individual certificates and apply them to the individual servers.

Answer: B

Question #:299 - (Exam Topic 1)

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts

B. Zero-day

C. Shared tenancy

D. Insider threat

Answer: D

Explanation

Insider Threat

An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

Additionally, these insiders don't even need to have malicious intentions.

A study by Imperva, "Inside Track on Insider Threats" found that an insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controling access, and implementing technology.

Question #:300 - (Exam Topic 1)

Which of the following is the purpose of an industry-standard framework?

A. To promulgate compliance requirements for sales of common IT systems

B. To provide legal relief to participating organizations in the event of a security breach

C. To promulgate security settings on a vendor-by-vendor basis

D. To provide guidance across common system implementations

Answer: D

Question #:301 - (Exam Topic 1)

A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site. Which of the following would BEST resolve the issue?

A. OSCP

B. OID

C. PEM

D. SAN

Answer: A

Question #:302 - (Exam Topic 1)

An organization is updating its access control standards for SSL VPN login to include multifactor authentication The security administrator assigned to this project has been given the following guidelines to use when selecting a solution

• High security

• Lowest false acceptance rate

• Quick provisioning time for remote users and offshore consultants

Which of the following solutions will BEST fit this organization's requirements?

A. AES-256 key fobs

B. Software tokens

C. Fingerprint scanners

D. Iris scanners

Answer: B

Question #:303 - (Exam Topic 1)

Penetration testing is distinct from vulnerability scanning primarily because penetration testing:

A. leverages credentials scanning to obtain persistence.

B. involve multiple active exploitation technique

C. relies exclusively on passive exploitation attempts for pivoting

D. relies on misconfiguration of security controls.

Answer: B

Question #:304 - (Exam Topic 1)

A security administrator plans to conduct a vulnerability scan on the network to determine if system applications are up to date. The administrator wants to limit disruptions to operations but not consume too many resources. Which of the following types of vulnerability scans should be conducted?

A. Credentialed

B. Non-Intrusive

C. SYN

D. Port

Answer: B

Question #:305 - (Exam Topic 1)

An auditor is requiring an organization to perform real-time validation of SSL certificates Which of the following should the organization implement?

A. OCSP

B. CRL

C. CSR

D. KDC

Answer: C

Question #:306 - (Exam Topic 1)

The security office has had reports of increased tailgating in the datacenter. Which of the following controls should security put in place?

A. Mantrap

B. Cipher lock

C. Fingerprint scanner

D. Badge reader

Answer: A

Question #:307 - (Exam Topic 1)

A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap

B. Honeypot

C. Aggregation

D. Port mirror

Answer: A

Question #:308 - (Exam Topic 1)

A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH

B. SFTP

C. HTTPS

D. SNMP

Answer: A

Question #:309 - (Exam Topic 1)

A security analyst is asked to check the configuration of the company's DNS service on the server. Which of the following command line tools should the analyst use to perform the Initial assessment?

A. nslookup/dlg

B. tracert

C. ipconfig/ifconfig

D. tcpdump

Answer: B

Question #:310 - (Exam Topic 1)

A technician is installing a new SIEM and is configuring the system to count the number of times an event occurs at a specific logical location before the system takes action. Which of the following BEST describes the feature being configured by the technician?

A. Correlation

B. Aggregation

C. Event deduplication

D. Flood guard

Answer: A

Question #:311 - (Exam Topic 1)

A systems administrator just issued the ssh-keygen -t rsa command on a Linux terminal Which of the following BEST describes what the rsa portion of the command represents?

A. A key generation algorithm

B. A hashing algorithm

C. A public key infrastructure type

D. A certificate authority type

Answer: A

Question #:312 - (Exam Topic 1)

A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Select TWO)

A. Use a unique managed service account

B. Utilize a generic password for authenticating

C. Enable and review account audit logs

D. Enforce least possible privileges for the account

E. Add the account to the local administrator's group.

F. Use a guest account placed in a non-privileged users' group

Answer: A D

Question #:313 - (Exam Topic 1)

A security engineer deploys a certificate from a commercial CA to the RADIUS server for use with the EAP-TLS wireless network. Authentication is failing, so the engineer examines the certificate's properties:

```
Issuer: (A commercial CA)
Valid from: (yesterday's date)
Valid to: (one year from yesterday's date)
Subject: CN smithco.com
Public key: RSA (2048 bits)
Enhanced key usage: Client authentication (1.3.6.1.5.5.7.3.2)
Key usage: Digital signature, key encipherment (a0)
```

Which of the following is the MOST likely cause of the failure?

A. The certificate is missing the proper OID.

B. The certificate is missing wire-less authentication in key usage.

C. The certificate is self-signed.

D. The certificate has expired.

Answer: B

Question #:314 - (Exam Topic 1)

An administrator is beginning an authorized penetration test of a corporate network. Which of the following

tools would BEST assist in identifying potential attacks?

A. Netstat

B. Honey pot

C. Company directory

D. Nmap

Answer: D

Question #:315 - (Exam Topic 1)

A network administrator is configuring a honeypot in a company's DMZ To provide a method for hackers to access the system easily, the company needs to configure a plaintext authentication method that will send only the username and password to a service in the honeypot. Which of the following protocols should the company use?

A. OAuth

B. PAP

C. RADIUS

D. Shibboleth

Answer: B

Question #:316 - (Exam Topic 1)

During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to $20 million in damages for the cost of $30,000 a year. Which of the following risk response techniques has the company chosen?

A. Transference

B. Avoidance

C. Mitigation

D. Acceptance

Answer: A

Question #:317 - (Exam Topic 1)

A newly hired Chief Security Officer (CSO) is reviewing the company's IRP and notices the procedures for zero-day malware attacks are being poorly executed, resulting m the CSIRT failing to address and coordinate malware removal from the system. Which of the following phases would BEST address these shortcomings?

A. Identification

B. Lessons learned

C. Recovery

D. Preparation

E. Eradication

Answer: B

Question #:318 - (Exam Topic 1)

Which of the following enables a corporation to extend local security policies to corporate resources hosted in a CSP's infrastructure?

A. PKI

B. CRL

C. Directory services

D. CASB

E. VDI

Answer: D

Question #:319 - (Exam Topic 1)

A software development company needs to augment staff by hiring consultants for a high-stakes project The project has the following requirements:

• Consultants will have access to flighty confidential, proprietary data.

• Consultants will not be provided with company-owned assets.

• Work needs to start Immediately.

• Consultants will be provided with Internal email addresses for communications.

Which of the following solutions is the BEST method lor controlling data exfiltration during this project?

A. Require that all consultant activity be restricted to a secure VDI environment.

B. Require the consultants to sign an agreement stating they will only use the company-provided email address for communications during the project.

C. Require updated antivirus. USB blocking, and a host-based firewall on all consultant devices.

D. Require the consultants to conned to the company VPN when accessing confidential resources.

Answer: A

Question #:320 - (Exam Topic 1)

A technician is recommending preventive physical security controls for a server room. Which of the technician MOST likely recommend? (Select Two).

A. Geofencing

B. Video Surveillance

C. Protected cabinets

D. Mantrap

E. Key exchange

F. Authorized personnel signage

Answer: C D

Question #:321 - (Exam Topic 1)

Which of the following are disadvantages of full backups? (Select THREE)

A. They rely on other backups tor recovery

B. They require the most storage.

C. They demand the most bandwidth.

D. They have the slowest recovery time

E. They are impossible in virtual environments

F. They require on-site storage.

G. They are time-consuming to complete.

Answer: B C G

Question #:322 - (Exam Topic 1)

Which of the following is MOST likely happening?

A. A hacker attempted to pivot using the web server interface.

B. A potential hacker could be banner grabbing to determine what architecture is being used

C. The DNS is misconfigured for the server's IP address.

D. A server is experiencing DoS, and the request Is timing out.

Answer: A

Question #:323 - (Exam Topic 1)

Which of the following is the BEST example of a reputation impact identified during a risk assessment?

A. A bad software patch taking down the production systems.

B. A misconfigured firewall exposing intellectual properly to the internet.

C. An attacker defacing the e-commerce portal.

D. Malware collecting credentials for company bank accounts.

Answer: B

Question #:324 - (Exam Topic 1)

A company is deploying MFDs in its office to improve employee productivity when dealing with paperwork. Which of the following concerns is MOST likely to be raised as a possible security issue in relation Io these devices?

A. Sensitive scanned materials being saved on the local hard drive

B. Faulty printer drivers causing PC performance degradation

C. Improperly congured NIC settings interfering with network security

D. Excessive disk space consumption due to storing large documents

Answer: B

Question #:325 - (Exam Topic 1)

Which of the following types of vulnerability scans typically returns more detailed and thorough insights into actual system vulnerabilities?

A. Non-credentialed

B. Intrusive

C. Credentialed

D. Non-Intrusive

Answer: B

Question #:326 - (Exam Topic 1)

The SOC is reviewing processes and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

A. Updating the playbooks with better decision points

B. Dividing the network into trusted and untrusted zones

C. Providing additional end-user training on acceptable use

D. Implementing manual quarantining of infected hosts

Answer: C

Question #:327 - (Exam Topic 1)

A coffee company, which operates a chain of stores across a large geography area is deploying tablets to use as port-of-sale devices A security consultant has been given the following requirements:

• The cashiers must be able to log in to the devices quickly.

• The devices must be compliant with applicable regulations for credit card usage

• The risk of loss or theft of the devices must be minimized

• If devices are lost or stolen, all data must be removed from the device

• The devices must be capable of being managed from a centralized location

Which of the following should the security consultant configure in the MDM policies for the tablets? (Select TWO)

A. Remote wipe

B. Cable locks

C. Screen locks

D. Geofencing

E. GPS tagging

F. Carrier unlocking

Answer: A B

Question #:328 - (Exam Topic 1)

A company has drafted an Insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs

B. Developing mandatory training to educate employees about the removable media policy

C. Implementing a group policy to block user access to system files

D. Blocking removable-media devices and write capabilities using a host-based security tool

Answer: B

Question #:329 - (Exam Topic 1)

An attacker has gained control of several systems on the Internet and is using them to attach a website, causing it to stop responding to legitimate traffic Which of the following BEST describes the attack?

A. MITM

B. DNS poisoning

C. Buffer overflow

D. DDoS

Answer: D

Question #:330 - (Exam Topic 1)

An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation

B. Steganography

C. Diffusion

D. BCRYPT

Answer: B

Question #:331 - (Exam Topic 1)

A common asymmetric algorithm utilizes the user's login name to create the key to encrypt communications. To ensure the key is Afferent each time the user encrypts data which of the following should be added to the login name?

A. PGP

B. Nonce

C. PSK

D. Certificate

Answer: B

Question #:332 - (Exam Topic 1)

A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust

B. UEFI

C. Supply chain

D. TPM

E. Crypto-malware

F. ARP poisoning

Answer: C

Question #:333 - (Exam Topic 1)

A company recently experienced a network security breach and wants to apply two-factor authentication to secure its network. Which of the following should the company use? (Select TWO)

A. User ID and password

B. Cognitive password and OTP

C. Fingerprint scanner and voice recognition

D. Smart card and PIN

E. Proximity card and CAC

Answer: B E

Question #:334 - (Exam Topic 1)

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical

B. Detective

C. Preventive

D. Compensating

Answer: D

Explanation

Preventative

Preventative controls are designed to be implemented prior to a threat event and reduce and/or avoid the likelihood and potential impact of a successful threat event. Examples of preventative controls include policies, standards, processes, procedures, encryption, firewalls, and physical barriers.

Detective

Detective controls are designed to detect a threat event while it is occurring and provide assistance during investigations and audits after the event has occurred. Examples of detective controls include security event log monitoring, host and network intrusion detection of threat events, and antivirus identification of malicious code.

Corrective

Corrective controls are designed to mitigate or limit the potential impact of a threat event once it has occurred and recover to normal operations. Examples of corrective controls include automatic removal of malicious code by antivirus software, business continuity and recovery plans, and host and network intrusion prevention of threat events.

Question #:335 - (Exam Topic 1)

During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.

B. Create and apply microsegmentation rules.

C. Emulate the malware in a heavily monitored DMZ segment.

D. Apply network blacklisting rules for the adversary domain.

Answer: B

Question #:336 - (Exam Topic 1)

A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection

B. Honeypots

C. Next-generation firewall

D. Penetration test

Answer: B

Question #:337 - (Exam Topic 1)

An organization uses an antivirus scanner from Company A on its firewall, an email system antivirus scanner from Company B. and an endpoint antivirus scanner from Company C. This is an example of:

A. unified threat management.

B. an OVAL system.

C. vendor diversity.

D. alternate processing sites.

Answer: C

Question #:338 - (Exam Topic 1)

A company's MOM policy outlines the following requirements:

• Devices can be securely sanitized.

• Devices must only utilize secure WiFi.

• Devices must have biometric and PIN code setup.

The employees must also agree that all devices set up within the MDM have location services turned on. Which of the following options will address AT LEAST two of these requirements?

A. Geofencing, CYOO

B. Geolocation. remote wipe

C. Full-device encryption, sideloading

BYOO. geolocation

Answer: B

Question #:339 - (Exam Topic 1)

Which of the following control types would a backup of server data provide in case of a system issue?

A. Corrector

B. Deterrent

C. Preventive

D. Detective

Answer: A

Question #:340 - (Exam Topic 1)

Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain

B. Notoriety

C. Political expression

D. Corporate espionage

Answer: B

Question #:341 - (Exam Topic 1)

A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. tcpdump

B. Protocol analyzer

C. Netstat

D. Nmap

Answer: D

Question #:342 - (Exam Topic 1)

A network administrator wants to gather information on the security of the network servers in the DMZ. The administrator runs the following command:

```
Telnet www.example.com 80
```

Which of the following actions is the administrator performing?

A. Grabbing the web server banner

B. Logging into the web server

C. Harvesting cleartext credentials

D. Accessing the web server management console

Answer: A

Question #:343 - (Exam Topic 1)

A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administrator use?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 10

Answer: D

Explanation

RAID 10, also known as **RAID** 1+0, is a **RAID** configuration that combines disk mirroring and disk striping to protect data. It requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved.

Question #:344 - (Exam Topic 1)

A Chief Executive Officer (CEO) is staying at a hotel during a business trip. The hotel's wireless network does not show a lock symbol. Which of the following precautions should the CEO take? (Select TWO).

A. Change the connection type to WPA2.

B. Change TKIP to CCMR

C. Use a VPN.

D. Tether to a mobile phone.

E. Create a tunnel connection with EAP-TTLS.

Answer: C E

Question #:345 - (Exam Topic 1)

An organization is setting up a satellite office and wishes to extend the corporate network to the new site. Which of the following is the BEST solution to allow the users to access corporate resources while focusing on usability and security?

A. Federated services

B. Single sign-on

C. Site-to-site VPN

D. SSL accelerators

Answer: C

Question #:346 - (Exam Topic 1)

Employees receive a benefits enrollment email from the company's human resources department at the beginning of each year. Several users have reported receiving the email but are unable to log in to the website with their usernames and passwords. Users who enter the URL for the human resources website can log in without issue. Which of the following security issues is occurring?

A. Several users' computers were not configured to use HTTPS to access the website.

B. The human resources servers received a large number of requests resulting in a DoS

C. The internal DNS server was compromised, directing users to a hacker's server.

D. Users received a social engineering email and were directed to an external website.

Answer: D

Question #:347 - (Exam Topic 1)

An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment

B. CYOD model

C. DAC model

D. BYOD model

Answer: B

Question #:348 - (Exam Topic 1)

An organization has the following written policies:

• Users must request approval for non-standard software installation

• Administrators will perform all software installations

• Software must be installed from a trusted repository

A recent security audit identified crypto-currency software installed on one user's machine There are no indications of compromise on this machine Which of the following is the MOST likely cause of this policy violation and the BEST remediation to prevent a reoccurrence'?

A. The user's machine was infected with malware implement the organization's incident response

B. The user installed the software on the machine implement technical controls to enforce the written policies

C. The crypto-currency software was misidentified and is authorized; add the software to the organization's approved list

D. Administrators downloaded the software from an untrusted repository; add a policy that requires integrity checking for all software

Answer: C

Question #:349 - (Exam Topic 1)

A network administrator needs to restrict the users of the company's WAPs to the sales department. The network administrator changes and hides the SSID and then discovers several employees had connected their personal devices to the wireless network. Which of the following would limit access to the wireless network to only organization-owned devices in the sales department?

A. Implementing MAC filtering

B. Reducing the signal strength to encompass only the sales department

C. Replacing the APs and sales department wireless cards to support 802.11b

D. Issuing a BYOD policy

Answer: A

Question #:350 - (Exam Topic 1)

A security engineer is concerned about susceptibility to HTTP downgrade attacks because the current

customer portal redirects users from port 80 to the secure site on port 443. Which of the following would be MOST appropriate to mitigate the attack?

A. DNSSEC

B. HSTS

C. Certificate pinning

D. OCSP

Answer: B

Question #:351 - (Exam Topic 1)

Which of the following involves the use of targeted and highly crafted custom attacks against a population of users who may have access to a particular service or program?

A. Hoaxing

B. Spear phishing

C. Vishing

D. Phishing

Answer: A

Question #:352 - (Exam Topic 1)

An engineer is configuring a wireless network using PEAP for the authentication protocol. Which of the following is required?

A. 802.11n support on the WAP

B. X.509 certificate on the server

C. CCMP support on the network switch

D. TLS 1.0 support on the client

Answer: B

Question #:353 - (Exam Topic 1)

As a security measure, an organization has disabled all external media from accessing the network Since some users may have data that needs to be transferred to the network, which of the would BEST assist a security

administrator with transferring the data while keeping the internal network secure?

A. Upload the media in the DMZ

B. Upload the data in a separate VLAN

C. Contact the data custodian

D. Use a standalone scanning system

Answer: A

Question #:354 - (Exam Topic 1)

An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting

B. Clickjacking

C. Buffer overflow

D. Replay

Answer: C

Question #:355 - (Exam Topic 1)

A systems administrator is receiving multiple alerts from the company NIPS. A review of the NIPS logs shows the following:

reset both: 70.32.200.2:3194 –> 10.4.100.4:80 buffer overflow attempt

reset both: 70.32.200.2:3230 –> 10.4.100.4:80 directory traversal attack

reset client: 70.32.200.2:4019 –> 10.4.100.4:80 Blind SQL injection attack

Which of the following should the systems administrator report back to management?

A. The company web server was attacked by an external source, and the NIPS blocked the attack.

B. The company web and SQL servers suffered a DoS caused by a misconfiguration of the NIPS.

C. An external attacker was able to compromise the SQL server using a vulnerable web application.

D. The NIPS should move from an inline mode to an out-of-band mode to reduce network latency.

Answer: A

Question #:356 - (Exam Topic 1)

A security consultant is analyzing data from a recent compromise. The following data points are documented

- Access to data on share drives and certain networked hosts was lost after an employee logged in to an interactive session as a privileged user.
- The data was unreadable by any known commercial software.
- The issue spread through the enterprise via SMB only when certain users accessed data.
- Removal instructions were not available from any major antivirus vendor.

Which of the following types of malware is this example of‘?

A. RAT

B. Ransomware

C. Backdoor

D. Keylogger

E. Worm

Answer: A

Question #:357 - (Exam Topic 1)

A security administrator is investigating a report that a user is receiving suspicious emails. The user’s machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Choose two.)

A. Vishing

B. Whaling

C. Spear phishing

D. Pharming

E. War dialing

F. Hoaxing

Answer: E F

Question #:358 - (Exam Topic 1)

Which of the following help find current and future gaps in an existing COOP?

A. Vulnerability assessment

B. Lessons learned

C. Tabletop exercise

D. After-action report

Answer: D

Question #:359 - (Exam Topic 1)

An organization is looking to build its second head ofce in another city. which has a history of ooding with an average of two oods every ‘I00 years. The estimated building cost is $1 million. and the estimated damage due to flooding is half of the buildings cost. Given this information, which of the following is the SLE?‘

A. $50,000

B. $200000

C. $500,000

D. $1.000000

Answer: C

Question #:360 - (Exam Topic 1)

An organization’s policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.

The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation.

Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements.

B. The password history enforcement is insufficient, and old passwords are still valid across many different

systems.

C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems.

D. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.

Answer: D

Explanation

Section: (none)

Explanation

Question #:361 - (Exam Topic 1)

A security administrator wants to better prepare the incident response team for possible security events. The IRP has been updated and distributed to incident response team members. Which of the following is the BEST option to fulfill the administrator's objective?

A. identify the members' roles and responsibilities.

B. Select a backup/failover location.

C. Determine the order of restoration.

D. Conduct a tabletop test.

Answer: A

Question #:362 - (Exam Topic 1)

A company is implementing a remote access portal so employees can work remotely from home. The company wants to implement a solution that would securely integrate with a third party. Which of the following is the BEST solution?

A. SAML

B. RADIUS

C. Secure token

D. TACACS+

Answer: B

Question #:363 - (Exam Topic 1)

Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites

B. Improper input handling

C. DLL injection

D. Certificate signing flaws

Answer: B

Question #:364 - (Exam Topic 1)

A salesperson often uses a USB drive to save and move files from a corporate laptop. The corporate laptop was recently updated, and now the files on the USB are read-only. Which of the following was recently added to the laptop?

A. Antivirus software

B. File integrity check

C. HIPS

D. DLP

Answer: D

Question #:365 - (Exam Topic 1)

Which of the following would have the GREATEST impact on the supporting, database server if input handling is not properly implemented on a web application?

A. Server-side request forgery

B. Cross-site request forgery

C. Insecure direct object reference

D. Command injection

E. Cross-site scripting

Answer: D

Question #:366 - (Exam Topic 1)

A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following methods should the technician use?

Shredding

A. Shredding

B. Low-level formatting

C. Repartitioning

D. Overwriting

Answer: A

Question #:367 - (Exam Topic 1)

A security administrator is reviewing the following information from a file that was found on a compromised host:

```
cat suspiciousfile.txt
www.CompTIA.org\njohn\miloveyou\n$200\nWorking Late\nJohn\nI%20will%20be%20in%20the%20office%20till%206pm%20to%20finish%20the%20report\n
```

Which of the following types of malware is MOST likely installed on the compromised host?

A. Keylogger

B. Spyware

C. Trojan

D. Backdoor

E. Rootkit

Answer: C

Question #:368 - (Exam Topic 1)

Proprietary information was sent by an employee to a distribution list that included external email addresses. Which of the following BEST describes the incident that occurred and the threat actor in this scenario?

A. Social engineering by a hacktivist

B. MITM attack by a script kiddle

C. Unintentional disclosure by an insider

D. Corporate espionage by a competitor

Answer: C

Question #:369 - (Exam Topic 1)

After a ransomware attack. a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

A. The public ledger

B. The NetFlow data

C. A checksum

D. The event log

Answer: D

Question #:370 - (Exam Topic 1)

Ann. a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot-up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann's computer?

A. The hard drive is falling, and the files are being corrupted.

B. The computer has been infected with crypto-malware.

C. A replay attack has occurred.

D. A keylogger has been installed.

Answer: B

Question #:371 - (Exam Topic 1)

A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configuration should the engineer choose?

A. EAP-TLS

B. EAP-TTLS

C. EAP-FAST

D. EAP-MD5

E. PEAP

Answer: A

Explanation

EAP-TLS uses the **TLS** public key certificate **authentication** mechanism within **EAP** to provide **mutual authentication** of **client** to **server** and **server** to **client**. With **EAP-TLS**, **both** the **client** and the **server** must be assigned a digital certificate signed by a Certificate Authority (CA) that they **both** trust.

Question #:372 - (Exam Topic 1)

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing

B. VM escape

C. Software-defined networking

D. Image forgery

E. Container breakout

Answer: B

Question #:373 - (Exam Topic 1)

Which of the following cloud models is used to share resources and information with business partners and like businesses without allowing everyone else access?

A. Public

B. Hybrid

C. Community

D. Private

Answer: C

Question #:374 - (Exam Topic 1)

A security analyst has identified malware that is propagating automatically to multiple systems on the network. Which of the following types of malware is MOST likely impacting the network?

A. Virus

B. Worm

C. Logic bomb

D. Backdoor

Answer: B

Question #:375 - (Exam Topic 1)

A technician is configuring an intrusion prevention system to improve its ability to find and stop threats In the past, the system did not detect and stop some threats Which of the following BEST describes what the technician is trying to correct with the new configuration?

A. False positives

B. False acceptance rate

C. False negatives

D. Error correction rate

E. False rejection rate

Answer: C

Question #:376 - (Exam Topic 1)

An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware

B. Logic bomb

C. Rootkit

D. Adware

Answer: C

Question #:377 - (Exam Topic 1)

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

Answer: D

Question #:378 - (Exam Topic 1)

A systems administrator recently issued a public/private key pair that will be used for the company's DNSSEC implementation Which of the following configurations should the systems administrator implement NEXT?

A. Create DNSKEY resources with the public key.

B. instant private key using the RRSIG record

C. Point the OS record to the company authoritative servers

D. Add TCP port 443 to the DNS listener

Answer: A

Question #:379 - (Exam Topic 1)

The website of a bank that an organization does business with is being reported as untrusted by the organization's web browser. A security analyst has been assigned to Investigate. The analyst discovers the band recently merged with another local bank and combined names. Additionally, the user's bookmark automatically redirects to the website of the newly named bank. Which of the following Is the MOST likely cause of the Issue?

A. The company's web browser is not up to date

B. The website's certificate still has the old bank's name.

C. The website was created too recently to be trusted.

D. The website's certificate has expired

Answer: C

Question #:380 - (Exam Topic 1)

When an initialization vector is added to each encryption cycle, it is using the:

A. ECB cipher mode.

B. MD5 cipher mode.

C. XOR cipher mode.

D. CBC cipher mode.

Answer: C

Question #:381 - (Exam Topic 1)

A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited information pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box

B. Gray box

C. White box

D. Vulnerability scanning

Answer: B

Question #:382 - (Exam Topic 1)

A computer forensics team is performing an integrity check on key systems files. The team is comparing the signatures of original baseline les with the latest signatures. The original baseline was taken on March 2, 2016. and was established to be clean of malware and uncorrupted. The latest tile signatures were generated yesterday. One file is known to be corrupted, but when the team compares the signatures of the original and latest ies, the team sees the

Following:

Original: 2d da b1 4a fc f1 98 06 b1 e5 26 b2 df e5 5b 3e cb 83 e1

Latest: 2d da b1 4a 98 fc f1 98 bl e5 26 b2 df e5 5b 3e cb 83 e1

Which of the following is MOST likely the situation?

A. The forensics team must have reverted the system to the original date. Which resulted in an identical hash calculation?

B. The original baseline was compromised, so the corrupted le was always on the system.

C. The signature comparison is using two different algorithms that happen to have generated the same values.

D. The algorithm used to calculate the hash has a collision weakness, and an attacker has exploited it.

Answer: D

Question #:383 - (Exam Topic 1)

A company recently contracted a penetration testing firm to conduct an assessment. During the assessment, the penetration testers were able to capture unencrypted communication between directory servers. The penetration testers recommended encrypting this communication to fix the vulnerability. Which of the following protocols should the company implement to close this finding?

A. DNSSEC

B. SFTP

C. Kerberos

D. LDAPS

Answer: D

Explanation

attacker captured LDAP communications. And secure version of LDAP is LDAPS(LDAP+TLS)

Question #:384 - (Exam Topic 1)

A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attack?

A. Brute force

B. Known plaintext

C. Replay

D. Collision

Answer: D

Question #:385 - (Exam Topic 1)

A vulnerability scan was run multiple times. The first lime, the scan detected multiple operating system flaws The second time the scan indicated that a few third-party application programs required patching and no operating system flaws. Which of the following is the MOST likely cause tor the different scan results?

A. The initial scan used credentials mat had limited access to system resources

B. The second scan used credentials that were configured for time-of-day scanning

C. The first scan had full-system scanning capabilities

D. The vulnerability scanner was not configured with the common vulnerability and exposure database

Answer: D

Question #:386 - (Exam Topic 1)

A pass-the-hash attack is commonly used to:

A. modify DNS records to point to a different domains.

B. modify the IP address of the targeted computer.

C. execute java script to capture user credentials.

D. laterally move across the network.

Answer: D

Question #:387 - (Exam Topic 1)

Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.

B. The vulnerability scanner is able to inventory software on the target.

C. A scan will reveal data loss in real time.

D. Black-box testing can be performed.

Answer: B

Question #:388 - (Exam Topic 1)

An internal intranet site is required to authenticate users and restrict access to content to only those who are authorized to view it The site administrator previously encountered issues with credential spoofing when using the default NTLM setting and wants to move to a system that will be more resilient to replay attacks Which of the following should the administrator implement?

A. NTLMv2

B. TACACS+

C. Kerberos

D. Shibboleth

Answer: B

Question #:389 - (Exam Topic 1)

Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation.

B. It enables system rollback to a last known-good state if patches break functionality.

C. It facilitates fault tolerance since applications can be migrated across templates.

D. It improves vulnerability scanning efficiency across multiple systems.

Answer: C

Question #:390 - (Exam Topic 1)

Which of the following controls does a mantrap BEST represent?

A. Deterrent

B. Detective

C. Physical

D. Corrective

Answer: C

Question #:391 - (Exam Topic 1)

A system uses an application server and database server Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server. Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).

The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit. Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.

B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application

servers.

C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.

D. Give the business unit administrative privileges on both the database and application servers so they can Independently monitor server activity.

Answer: A

Question #:392 - (Exam Topic 1)

A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap

B. Network proxy

C. Honeypot

D. Port mirroring

Answer: A

Explanation

Port Mirroring, also known as SPAN (Switched Port Analyzer), is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.

Question #:393 - (Exam Topic 1)

A systems administrator has created network file shares for each department with associated security groups for each role within the organization. Which of the following security concepts is the systems administrator implementing?

A. Separation of duties

B. Permission auditing

C. Least privilege

D. Standard naming convention

Answer: A

Question #:394 - (Exam Topic 1)

An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE

B. ARO

C. RPO

D. SLE

Answer: D

Question #:395 - (Exam Topic 1)

A security administrator found the following piece of code referenced on a domain controller's task scheduler:

$var = GetDomainAdmins

If $var != ‘fabio’

SetDomainAdmins = NULL

With which of the following types of malware is the code associated?

A. RAT

B. Backdoor

C. Logic bomb

D. Crypto-malware

Answer: C

Question #:396 - (Exam Topic 1)

A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Select TWO).

A. Implement time-of-day restrictions.

B. Modify archived data.

C. Access executive shared portals.

D. Create privileged accounts.

E. Enforce least privilege.

Answer: A D

Question #:397 - (Exam Topic 1)

Which of the following is the security threat a hiring manager is trying to prevent by performing a background screening of a job candidate?

A. Plagiansm

B. Open-source intelligence

C. Malicious insider

D. Social engineering

E. Hacktivtsm

Answer: C

Question #:398 - (Exam Topic 1)

Which of the following is an algorithm family that was developed for use cases in which power consumption and lower computing power are constraints?

A. Elliptic curve

B. RSA

C. Diffie-Hellman

D. SHA

Answer: A

Question #:399 - (Exam Topic 1)

The Chief information Officer (CIO) has decided to add two-factor authentication along with the use of passwords when logging on to the network. Which of the following should be implemented to BEST accomplish this requirement?

A Require users to enter a PIN

B Require users to set complex passwords

C. Require users to insert a smart card when logging on

D. Require the system to use a CAPTCHA

C

Question #:400 - (Exam Topic 1)

Some call center representatives 'workstations were recently updated by a contractor, who was able to collect customer information from the call center workstations. Which of the following types of malware was installed on the call center users' systems?

A. Adware

B. Logic bomb

C. Trojan

D. Spyware

Answer: D

Question #:401 - (Exam Topic 1)

An email recipient is unable to open a message encrypted through PKI that was sent from another organization. Which of the following does the recipient need to decrypt the message?

A. The sender's private key

B. The recipient's private key

C. The recipient's public key

D. The CA's root certificate

E. The sender's public key

F. An updated CRL

Answer: E

Question #:402 - (Exam Topic 1)

Which of the following encryption algorithms require one encryption key? (Choose two.)

A. MD5

B. 3DES

C. BCRYPT

D. RC4

E. DSA

Answer: B D

Question #:403 - (Exam Topic 1)

During incident response procedures, technicians capture a unique identifier for a piece of malware running in memory. This captured information is referred to as:

A. a hash value.

B. the SSID.

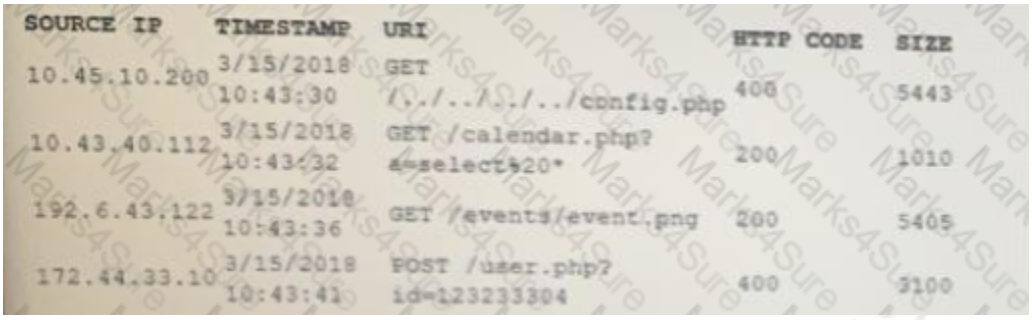
C. the GUID.

D. a system image.

Answer: A

Question #:404 - (Exam Topic 1)

An analyst is reviewing the following web-server log after receiving an alert from the DLP system about multiple PII records being transmitted in cleartext:



SOURCE IP	TIMESTAMP	URI	HTTP CODE	SIZE
10.45.10.200	3/15/2018 10:43:30	GET /../../../../config.php	400	5443
10.43.40.112	3/15/2018 10:43:32	GET /calendar.php?a=select%20*	200	1010
192.6.43.122	3/15/2018 10:43:36	GET /events/event.png	200	5405
172.44.33.10	3/15/2018 10:43:41	POST /user.php?id=123233304	400	3100

Which of the following IP addresses in MOST likely involved in the data leakage attempt?

A. 10.43.40.112

B. 10.45.10.200

C. 172.44.33.10

D. 192.4.43.122

Answer: C

Question #:405 - (Exam Topic 1)

A security administrator is investigating a possible account compromise. The administrator logs onto a desktop computer, executes the command notepad.exe c:\Temp\qkakforlkgfkja.1og, and reviews the following:

Lee,\rI have completed the task that was assigned to me\rrespectfully\rJohn\r

https://www.portal.com\rjohnuser\rilovemycat2

Given the above output, which of the following is the MOST likely cause of this compromise?

A. Virus

B. Worm

C. Rootkit

D. Keylogger

Answer: D

Question #:406 - (Exam Topic 1)

A technician is implementing 802 1X with dynamic VLAN assignment based on a user Active Directory group membership Which of the following configurations supports the VLAN definitions?

A. RADIUS attribute

B. SAML tag

C. LDAP path

D. Shibboleth IdP

Answer: B

Question #:407 - (Exam Topic 1)

After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:

Rule #	Source	Destination	Port(s)	Protocol	Action	Hit Count
13	192.168.1.99	10.5.10.254	80, 443, 53	TCP	ALLOW	0
27	192.168.1.99	10.5.10.254	5799,5798,5800	UDP	ALLOW	916
999	192.168.1.0/24	ANY	ANY	TCP, UDP	DENY	10988

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled

B. The VLAN is not trunked properly

C. There is a policy violation for DNS lookups

D. The firewall policy is misconfigured

Answer: D

Question #:408 - (Exam Topic 1)

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. dd

B. chmod

C. dnaenum

D. logger

Answer: A

Question #:409 - (Exam Topic 1)

A security engineer wants to further secure a sensitive VLAN on the network by introducing MFA. Which of the following is the BEST example of this?

A. PSK and PIN

B. RSA token and password

C. Fingerprint scanner and voice recognition

D. Secret question and CAPTCHA

Answer: B

Question #:410 - (Exam Topic 1)

An administrator needs to protect rive websites with SSL certificates Three of the websites have different domain names, and two of the websites share the domain name but have different subdomain prefixes. Which of the following SSL certificates should the administrator purchase to protect all the websites and be able to administer them easily at a later time?

A. One SAN certificate

B. One Unified Communications Certificate and one wildcard certificate

C. One wildcard certificate and two standard certificates

D. Five standard certificates

Answer: B

Question #:411 - (Exam Topic 1)

A company moved into a new building next to a sugar mil. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational

B. Man-made

C. Environmental

D. Natural

Answer: A

Question #:412 - (Exam Topic 1)

An analyst is currently looking at the following output:

Software Name	Status	Licensed	Used
Software 1	Approved	100	91
Software 2	Approved	50	52
Software 3	Approved	100	87
Software 4	Approved	50	46
Software 5	Denied	0	0

Which of the following security issues has been discovered based on the output?

A. Insider threat

B. License compliance violation

C. Unauthorized software

D. Miscongured admin permissions

Answer: B

Question #:413 - (Exam Topic 1)

An organization wants to control user accounts and privileged access to database servers. The organization wants to create an audit trail of account requests and approval. but also wants to facilitate operational efficiency when account and access changes are needed. The organization has the following account management practices:

Which of the following should the security consultant configure in the MDM policies for the tables? (Select TWO.)

A. Remote wipe

B. Cable locks

C. Screen locks

D. Geofencing

E. GPS tagging

F. Carrier unlocking

Answer: A D

Topic 2, Exam Pool B

Question #:1 - (Exam Topic 2)

A company has a team of penetration testers. This team has located a file on the company file server that they believe contains cleartext usernames followed by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework

B. Vulnerability scanner

C. Netcat

D. Password cracker

Answer: D

Question #:2 - (Exam Topic 2)

The Chief Information Officer (CIO) has determined the company's new PKI will not use OCSP. The purpose of OCSP still needs to be addressed. Which of the following should be implemented?

A. Build an online intermediate CA.

B. Implement a key escrow.

C. Implement stapling.

D. Install a CRL.

Answer: D

Question #:3 - (Exam Topic 2)

A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0

B. RAID 1

C. RAID 2

D. RAID 3

Answer: B

Question #:4 - (Exam Topic 2)

After patching computers with the latest application security patches/updates, users are unable to open certain applications. Which of the following will correct the issue?

A. Modifying the security policy for patch management tools

B. Modifying the security policy for HIDS/HIPS

C. Modifying the security policy for DLP

D. Modifying the security policy for media control

Answer: C

Question #:5 - (Exam Topic 2)

A manager makes an unannounced visit to the marketing department and performs a walk-through of the office. The manager observes unclaimed documents on printers. A closer look at these documents reveals employee names, addresses, ages, birth dates, marital/dependent statuses, and favorite ice cream flavors. The manager brings this to the attention of the marketing department head. The manager believes this information to be PII, but the marketing head does not agree. Having reached a stalemate, which of the following is the MOST appropriate action to take NEXT?

A. Elevate to the Chief Executive Officer (CEO) for redress; change from the top down usually succeeds.

B. Find the privacy officer in the organization and let the officer act as the arbiter.

C. Notify employees whose names are on these files that their personal information is being compromised.

D. To maintain a working relationship with marketing, quietly record the incident in the risk register.

Answer: B

Question #:6 - (Exam Topic 2)

A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege

B. External intruder

C. Conflict of Interest

D. Fraud

Answer: A

Explanation

The **principle of least privilege** works by allowing only enough access to perform the required job. In an IT environment, adhering to the **principle of least privilege** reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.

Question #:7 - (Exam Topic 2)

Using a one-time code that has been texted to a smartphone is an example of:

A. something you have.

B. something you know.

C. something you do.

D. something you are.

Answer: A

Question #:8 - (Exam Topic 2)

In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting

B. To minimize signal attenuation over distances to maximize signal strength

C. To minimize external RF interference with embedded processors

D. To protect the integrity of audit logs from malicious alteration

Answer: C

Question #:9 - (Exam Topic 2)

Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Select TWO).

A. Accounting

B. Authentication

C. Auditing

D. Authorization

E. Non-repudiation

Answer: A C

Question #:10 - (Exam Topic 2)

An Organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.

The application team receive a report with the following results:

Host	Environment	Baseline deviation ID (criticality)
NYAccountingDev	Development	
NYAccountingStg	Staging	
NYAccountingProd	Production	2633 (low), 3124 (high)

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate If the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?

A. Remediate 2633 and 3124 immediately.

B. Process a risk acceptance for 2633 and 3124.

C. Process a risk acceptance for 2633 and remediate 3124.

D. Shut down NYAccountingProd and Investigate the reason for the different scan results.

Answer: C

Question #:11 - (Exam Topic 2)

A coffee company has hired an IT consultant to set up a WiFi network that will provide Internet access to customers who visit the company's chain of cafés. The coffee company has provided no requirements other than that customers should be granted access after registering via a web form and accepting the terms of

service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?

A. Captive portal

B. WPA with PSK

C. Open WiFi

D. WPS

Answer: A

Explanation

A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.

Question #:12 - (Exam Topic 2)

A security administrator is adding a NAC requirement for all VPN users to ensure the co requirement?

A. Implement a permanent agent.

B. Install antivirus software.

C. Use an agentless implementation.

D. Implement PKI.

Answer: A

Question #:13 - (Exam Topic 2)

Which of the following is the primary reason for implementing layered security measures in a cyber security architecture?

A. it increases the number of controls required to subvert a system.

B It decreases the tone a CERT has to respond to a security Incident.

B. It alleviates problems associated with EOL equipment replacement.

C. It allows for bandwidth upgrades to be made without user disruption.

Answer: B

Question #:14 - (Exam Topic 2)

A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A CVE

B. SIEM

C. SOAR

D. CVSS

C

Question #:15 - (Exam Topic 2)

A security consultant was asked to revise the security baselines that are utilized by a large organization. Although the company provides different platforms for its staff, including desktops, laptops, and mobile devices, the applications do not vary by platform. Which of the following should the consultant recommend? (Select Two).

A. Apply patch management on a daily basis.

B. Allow full functionality for all applications that are accessed remotely

C. Apply default configurations of all operating systems

D. Apply application whitelisting.

E. Disable default accounts and/or passwords.

Answer: A E

Question #:16 - (Exam Topic 2)

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Select TWO).

A. Data accessibility

B. Legal hold

C. Cryptographic or hash algorithm

D. Data retention legislation

E. Value and volatility of data

F. Right-to-audit clauses

Answer: C D

Question #:17 - (Exam Topic 2)

A systems administrator is configuring a new network switch for TACACS+ management and authentication.

Which of the following must be configured to provide authentication between the switch and the TACACS+ server?

A. 802.1X

B. SSH

C. Shared secret

D. SNMPv3

E. CHAP

Answer: C

Question #:18 - (Exam Topic 2)

A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID. Which of the following should the security administrator use to assess connectivity?

A. Sniffer

B. Honeypot

C. Routing tables

D. Wireless scanner

Answer: C

Question #:19 - (Exam Topic 2)

A company is having Issues with intellectual property being sent to a competitor from its system. The information being sent Is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop the content from being sent?

A. Encryption

B. Hashing

C. IPS

D. DLP

Answer: D

Question #:20 - (Exam Topic 2)

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat Intelligence data?

A. STIX

B. CIRT

C. OSINT

D. TAXII

Answer: B

Question #:21 - (Exam Topic 2)

A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal network securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. VPN

B. PaaS

C. IaaS

D. VDI

Answer: A

Question #:22 - (Exam Topic 2)

Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness

B. Zero-day

C. Logic bomb

D. Trojan

Answer: B

Question #:23 - (Exam Topic 2)

A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes. Which of the following configurations should the security administrator set up in order to complete this request?

A. LDAP

B. RADIUS

C. SAML

D. NTLM

Answer: B

Question #:24 - (Exam Topic 2)

Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not.

B. One has a higher potential for disrupting system operations.

C. One allows systems to activate firewall countermeasures.

D. One returns service banners, including running versions.

Answer: B

Question #:25 - (Exam Topic 2)

A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash attack

B. ARP poisoning attack

C. Birthday attack

D. Brute-force attack

Answer: A

Question #:26 - (Exam Topic 2)

A security administrator is analyzing a user report in which the computer exhibits odd network-related outages. The administrator, however, does not see any suspicious process running. A prior technician's notes indicate the machine has been remediated twice, but the system still exhibits odd behavior. Files were deleted from the system recently.

Which of the following is the MOST likely cause of this behavior?

A. Crypto-malware

B. Rootkit

C. Logic bomb

D. Session hijacking

Answer: B

Question #:27 - (Exam Topic 2)

Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

A. It allows the software to run in an unconstrained environment with full network access.

B. It eliminates the possibility of privilege escalation attacks against the local VM host.

C. It facilitates the analysis of possible malware by allowing it to run until resources are exhausted.

D. It restricts the access of the software to a contained logical space and limits possible damage.

Answer: D

Question #:28 - (Exam Topic 2)

Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive

B. Passive reconnaissance

C. Access violation

D. Privilege escalation

Answer: A

Question #:29 - (Exam Topic 2)

A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Select TWO).

A. Compare configurations against platform benchmarks,

B. Confirm adherence to the company's industry-specific regulations.

C. Review the company's current security baseline,

D. Verify alignment with policy related to regulatory compliance

E. Run an exploitation framework to confirm vulnerabilities

Answer: C E

Question #:30 - (Exam Topic 2)

During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive

B. RAM

C. Network attached storage

D. USB flash drive

Answer: B

Question #:31 - (Exam Topic 2)

A hospital has received reports from multiple patients that their PHI was stolen after completing forms on the hospital's website. Upon investigation, the hospital finds a packet analyzer was used to steal data. Which of the following protocols would prevent this attack from reoccurring?

A. SFTP

B. HTTPS

C. FTPS

D. SRTP

Answer: A

Explanation

FTPS (also known FTP-SSL, and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and, formerly, the Secure Sockets Layer (SSL, which is now prohibited by RFC7568) cryptographic protocols.

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication. HTTPS is specified by RFC 2818 (May 2000) and uses port 443 by default instead of HTTP's port 80.

The HTTPS protocol makes it possible for website users to transmit sensitive data such as credit card numbers, banking information, and login credentials securely over the internet. For this reason, HTTPS is especially important for securing online activities such as shopping, banking, and remote work. However, HTTPS is quickly becoming the standard protocol for all websites, whether or not they exchange sensitive data with users.

SFTP (SSH File Transfer Protocol) is a secure file transfer protocol. It runs over the SSH protocol. It supports the full security and authentication functionality of SSH. SFTP has pretty much replaced legacy FTP as a file transfer protocol, and is quickly replacing FTP/S.

SRTP (Secure Real-Time Transport Protocol or Secure RTP) is an extension to RTP (Real-Time Transport Protocol) that incorporates enhanced security features. Like RTP, it is intended particularly for VoIP (Voice over IP) communications.

Question #:32 - (Exam Topic 2)

An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements, and must also be able to log in to the headquarters location remotely. Which of the following BEST represent how the remote employees should have been set up initially? (Select TWO).

A. User-based access control

B. Shared accounts

C. Group-based access control

D. Mapped drives

E. Individual accounts

F. Location-based policies

Answer: C E

Question #:33 - (Exam Topic 2)

A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator Implement?

A. WPS

B. PEAP

C. TKIP

D. PKl

Answer: A

Question #:34 - (Exam Topic 2)

Which of the following access management concepts is MOST closely associated with the use of a password or PIN??

A. Authorization

B. Authentication

C. Accounting

D. Identification

Answer: B

Question #:35 - (Exam Topic 2)

Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving

B. Man-in-the-browser

C. Spear phishing

D. Watering hole

Answer: A

Question #:36 - (Exam Topic 2)

The network information for a workstation is as follows:

IP address/subnet mask	Default gateway	DNS server
172.16.17.200/24	172.16.17.254	172.16.17.254

When the workstation's user attempts to access www.example.com. the URL that actually opens is www.notexample.com. The user successfully connects to several other legitimate URLs. Which of the following have MOST likely occurred? (Select TWO).

A. ARP poisoning

B. Buffer overflow

C. DNS poisoning

D. Domain hijacking

E. IP spoofing

Answer: C D

Question #:37 - (Exam Topic 2)

Joe recently assumed the role of data custodian for this organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled “unclassified” and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

A. Burning

B. Wiping

C. Purging

D. Pulverizing

Answer: D

Question #:38 - (Exam Topic 2)

A systems administrator wants to replace the process of using a CRL to verify certificate validity. Frequent downloads are becoming problematic. Which of the following would BEST suit the administrator's needs?

A. OCSP

B. CSR

C. Key escrow

D. CA

Answer: A

Question #:39 - (Exam Topic 2)

In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility.

Which of the following describes the type of actors that may have been implicated?

A. Nation-state

B. Hacktivist

C. Insider

D. Competitor

Answer: A

Question #:40 - (Exam Topic 2)

After reading a security bulletin, a network security manager Is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code Is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output

B. The IDS logs

C. The full packet capture data

D. The SIEM alerts

Answer: A

Question #:41 - (Exam Topic 2)

Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicates an error

B. The vendor has not published security patches recently.

C. The object has been removed from the Active Directory.

D. Logs show a performance degradation of the component.

Answer: B

Question #:42 - (Exam Topic 2)

A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:

```
Proto  Local Address  Foreign Address     State
TCP    0.0.0.0:445                       Listening     RpcSs
TCP    0.0.0.0:80                        Listening     httpd.exe
TCP    0.0.0.0:443    192.168.1.20:1301  Established   httpd.exe
TCP    0.0.0.0:90328  172.55.80.22:9090  Established   notepad.exe
```

Based on the above information, which of the following types of malware should the technician report?

A. Spyware

B. Rootkit

C. RAT

D. Logic bomb

Answer: C

Question #:43 - (Exam Topic 2)

An Organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group.

B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.

C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made.

D. Assign file and folder permissions on an Individual user basis and avoid group assignment altogether.

Answer: A

Question #:44 - (Exam Topic 2)

A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the Internet?

A. VLAN

B. Air gap

C. NAT

D. Firewall

Answer: B

Explanation

An air gap, air wall or air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

Question #:45 - (Exam Topic 2)

In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99 999% availability of its web application

B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster

C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department

D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor not block, any traffic

E. A company purchased liability insurance for flood protection on all capital assets

Answer: A

Question #:46 - (Exam Topic 2)

A cybersecurity analyst needs to Implement secure authentication to third-party websites without users' passwords Which of the following would be the BEST way to achieve this objective?

A. OAuth

B. SSO

C. SAML

D. PAP

Answer: B

Question #:47 - (Exam Topic 2)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social-engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Answer: B

Question #:48 - (Exam Topic 2)

Which of the following is unique to a stream cipher?

A. It encrypts 128 bytes at a time.

B. It uses AES encryption

C. It performs bit-level encryption

D. It is used in HTTPS

Answer: C

Question #:49 - (Exam Topic 2)

During a penetration test, the tester performs a preliminary scan for any responsive hosts. Which of the

following BEST explains why the tester is doing this?

A. To determine if the network routes are improperly forwarding request packets

B. To identify the total number of hosts and determine if the network can be victimized by a DoS attack

C. To identify servers for subsequent scans and further investigation

D. To identify the unresponsive hosts and determine if those could be used as zombies in a follow-up scan.

Answer: C

Question #:50 - (Exam Topic 2)

When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware

B. Tight integration to existing systems

C. IP address exhaustion

D. Not using industry standards

Answer: B

Question #:51 - (Exam Topic 2)

A security analyst is hardening a large-scale wireless network. The primary requirements are the following

* Must use authentication through EAP-TLS certificates

* Must use an AAA server

* Must use the most secure encryption protocol

Given these requirements, which of the following should the analyst implement and recommend? (Select TWO).

A. 802.1X

B. 802.3

C. LDAP

D. TKIP

E. CCMP

F. WPA2-PSK

Answer: A F

Question #:52 - (Exam Topic 2)

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for Signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value: SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration

B. Create a blocking policy based on the parameter values

C. Change the parameter name 'Account_Name' identified in the log.

D. Create an alert to generate emails for abnormally high activity.

Answer: D

Question #:53 - (Exam Topic 2)

A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation

B. TLS host certificate

C. OCSP stapling

D. Wildcard certificate

Answer: D

Question #:54 - (Exam Topic 2)

During an audit, the auditor requests to see a copy of the identified mission-critical applications as well as their disaster recovery plans. The company being audited has an SLA around the applications it hosts. With which of the following is the auditor MOST likely concerned?

A. ARO/ALE

B. MTTR/MTBF

C. RTO/RPO

D. Risk assessment

Answer: C

Question #:55 - (Exam Topic 2)

A systems administrator wants to implement a secure wireless network requiring wireless clients to pre-register with the company and install a PKI client certificate prior to being able to connect to the wireless network. Which of the following should the systems administrator configure?

A. EAP-TTLS

B. EAP-TLS

C. EAP-FAST

D. EAP with PEAP

E. EAP with MSCHAPv2

Answer: B

Question #:56 - (Exam Topic 2)

An analyst has determined that a server was not patched and an external actor extiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?

A. The vulnerability scan output

B. The security logs

C. The baseline report

D. The correlation of events

Answer: B

Question #:57 - (Exam Topic 2)

A manufacturer creates designs for very high security products that are required to be protected and controlled by government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap

B. A Faraday cage

C. A shielded cable

D. A demilitarized zone

Answer: B

Question #:58 - (Exam Topic 2)

When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed a implement:

A. session keys.

B. encryption of data at rest

C. encryption of data in use.

D. ephemeral keys.

Answer: D

Explanation

Compromising data in use enables access to encrypted data at rest and data in motion. For example, someone with access to random access memory (RAM) can parse that memory to locate the encryption key for data at rest. Once they have obtained that encryption key, they can decrypt encrypted data at rest.

Question #:59 - (Exam Topic 2)

Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP

B. NDA

C. ISA

D. BPA

Answer: A

Question #:60 - (Exam Topic 2)

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:

The username you entered does not exist.

Which of the following should the analyst recommend be enabled?

A. Input validation

B. Obfuscation

C. Error handling

D. Username lockout

Answer: D

Question #:61 - (Exam Topic 2)

Which of the following BEST describes the purpose of authorization?

A. Authorization provides logging to a resource and comes after authentication.

B. Authorization provides authentication to a resource and comes after identification.

C. Authorization provides identification to a resource and comes after authentication.

D. Authorization provides permissions to a resource and comes after authentication.

Answer: D

Question #:62 - (Exam Topic 2)

An attacker has gathered information about a company employee by obtaining publicly available information from the Internet and social networks. Which of the following types of activity is the attacker performing?

A. Pivoting

B. Exfiltration of data

C. Social engineering

D. Passive reconnaissance

Answer: B

Question #:63 - (Exam Topic 2)

Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance

B. Pivoting

C. White box testing

D. Persistence

Answer: C

Question #:64 - (Exam Topic 2)

A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks forbase64 encoded strings and applies the filter http.authbasic. Which of the following describes what the analysts looking for?

A. Unauthorized software

B. Unencrypted credentials

C. SSL certificate issues

D. Authentication tokens

Answer: D

Question #:65 - (Exam Topic 2)

A company is planning to utilize its legacy desktop systems by converting them into dummy terminals and moving all heavy applications and storage to a centralized server that hosts all of the company's required desktop applications. Which of the following describes the BEST deployment method to meet these requirements?

A. IaaS

B. VM sprawl

C. VDI

D. PaaS

Answer: C

Question #:66 - (Exam Topic 2)

A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather this information?

A. DMZ

B. Guest network

C. Ad hoc

D. Honeynet

Answer: D

Question #:67 - (Exam Topic 2)

A company that processes sensitive information has implemented a BYOD policy and an MDM solution to secure sensitive data that is processed by corporate and personally owned mobile devices. Which of the following should the company implement to prevent sensitive data from being stored on mobile devices?

A. VDI

B. Storage segmentation

C. Containerization

D. USB OTG

E. Geofencing

Answer: B

Explanation

Storage segmentation: Storage segmentation offers a special feature whereby the user can artificially

categorize different types of data on a mobile device's storage media. By default, a device uses storage segmentation to divide the device's preinstalled apps and operating system from the user data and user-installed apps.

Question #:68 - (Exam Topic 2)

If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA

B. 3DES

C. DSA

D. SHA-2

Answer: D

Question #:69 - (Exam Topic 2)

A security analyst runs a monthly file integrity check on the main web server. When analyzing the logs, the analyst observed the following entry:

File	Previous hash	Current hash
cmd.exe	c4ca6a34c5e3a0f98dc03d4f8adf56a3	a24f5a34c5e3a0f98dc03d4f8ac5c0e2
iexplore.exe	b9c8e3f24b38c94a7c5f3d9d8d4e7ab3	b9c8e3f24b38c94a7c5f3d9d8d4e7ab3

No OS patches were applied to this server during this period. Considering the log output, which of the following is the BEST conclusion?

A. The cmd.exe was executed on the scanned server between the two dates. An incident ticket should be created

B. The iexplore.exe was executed on the scanned server between the two dates. An incident ticket should be created.

C. The cmd.exe was updated on the scanned server. An incident ticket should be created

D. The iexplore.exe was updated on the scanned server. An incident ticket should be created.

Answer: C

Question #:70 - (Exam Topic 2)

A security technician is configuring a new firewall appliance for a production environment. The firewall must support secure web services for client workstations on the 10.10.10.0/24 network. The same client workstations are configured to contact a server at 192.168.1.15/24 for domain name resolution. Which of the following rules should the technician add to the firewall to allow this connectivity for the client workstations? (Select TWO).

A. Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 22

B. Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 80

C. Permit 10.10.10.0/24192.168.1.15/24 -p udp --dport 21

D. Permit 10.10.10.0/24 0.0.0.0-p tcp --dport 443

E. Permit 10.10.10.0/24 192.168.1.15/24 -p tcp --dport 53

F. Permit 10.10.10.0/24 192.168.1.15/24 -p udp --dport 53

Answer: D E

Question #:71 - (Exam Topic 2)

After a security assessment was performed on the enterprise network, it was discovered that:

- Configuration changes have been made by users without the consent of IT.
- Network congestion has increased due to the use of social media.
- Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describe the vulnerabilities that exist in this environment? (Choose two.)

A. Poorly trained users

B. Misconfigured WAP settings

C. Undocumented assets

D. Improperly configured accounts

E. Vulnerable business processes

Answer: A D

Question #:72 - (Exam Topic 2)

A security engineer at a manufacturing company is implementing a third-party cloud application. Rather than creating users manually in the application, the engineer decides to use the SAML protocol. Which of the

following is being used for this implementation?

A. The manufacturing company is the service provider, and the cloud company is the identity provider.

B. The manufacturing company is the authorization provider, and the cloud company is the service provider.

C. The manufacturing company is the identity provider, and the cloud company is the OAuth provider.

D. The manufacturing company is the identity provider, and the cloud company is the service provider.

E. The manufacturing company is the service provider, and the cloud company is the authorization provider.

Answer: A

Question #:73 - (Exam Topic 2)

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO)

A. The order of volatility

B. A checksum

C. The location of the artifacts

D. The vendor's name

E. The date and time

F. A warning banner

Answer: B C

Question #:74 - (Exam Topic 2)

A security technician has been given the task of preserving emails that are potentially involved in a dispute between a company and a contractor.

Which of the following BEST describes this forensic concept?

A. Legal hold

B. Chain of custody

C. Order of volatility

D. Data acquisition

Answer: A

Question #:75 - (Exam Topic 2)

Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking

B. IP spoofing

C. Evil twin

D. ARP poisoning

Answer: D

Explanation

An **ARP spoofing**, also known as **ARP poisoning**, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows: The attacker must have access to the network.

Question #:76 - (Exam Topic 2)

Using an ROT13 cipher to protocol confidential information for unauthorized access is known as:

A. Steganography

B. Obfuscation

C. Non repudiation

D. diffusion

Answer: B

Question #:77 - (Exam Topic 2)

A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation

B. Identification

C. Containment

D. Eradication

E. Recovery

F. Lessons learned

Answer: E

Question #:78 - (Exam Topic 2)

The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.

B. Prevent data exposure queries.

C. Obfuscate the source code.

D. Submit the application to QA before releasing it.

Answer: C

Question #:79 - (Exam Topic 2)

A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

Time: 12/25 0300

From Zone: Untrust

To Zone: DMZ

Attacker: externalip.com

Victim: 172.16.0.20

To Port: 80

Action: Alert

Severity: Critical

When examining the PCAP associated with the event, the security administrator finds the following information:

<script> alert ("Click

here for important information regarding your account! http://externalip.com/account.php

"); </script>

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.

B. Manually copy the <script> data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.

C. Implement a host-based firewall rule to block future events of this type from occurring.

D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

Answer: B

Question #:80 - (Exam Topic 2)

Given the output:

Date/time	Computer name	User ID	Website
3-15-18 2:00	Officedesktop	CompanyUser	www.comptia.org
3-15-18 2:13	Officedesktop	CompanyUser	www.companysite.com
3-15-18 2:22	Officedesktop	CompanyUser	www.localbank.org
3-15-18 2:46	Officedesktop	CompanyUser	www.myschool.edu

Which of the following account management practices should the security engineer use to mitigate the identified risk?

A. Implement least privilege.

B. Eliminate shared accounts.

C. Eliminate password reuse.

D. Implement two-factor authentication.

Answer: B

Question #:81 - (Exam Topic 2)

A company is performing an analysis of which corporate units are most likely to cause revenue loss in the

event the unit is unable to operate. Which of the following is an element of the BIA that this action is addressing?

A. Critical system inventory

B. Single point of failure

C. Continuity of operations

D. Mission-essential functions

Answer: D

Question #:82 - (Exam Topic 2)

Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment

B. A DoS using loT devices

C. An evil twin wireless access point

D. A domain hijacking of a bank website

Answer: A

Question #:83 - (Exam Topic 2)

A security operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment

B. Chain of custody

C. Lessons learned

D. Penetration test

Answer: B

Question #:84 - (Exam Topic 2)

A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

A. Vulnerability feeds

B. Trusted automated exchange of indicator Information

C. Structured threat information expression

D. Industry Information-sharing and collaboration groups

Answer: A

Question #:85 - (Exam Topic 2)

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

A. openssl

B. hping

C. netcat

D. tcpdump

Answer: D

Question #:86 - (Exam Topic 2)

An employee workstation with an IP address of 204 211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

IP Address	Protocol	Port Number	Action
204.211.38.1/24	ALL	ALL	Permit
204.211.38.211/24	ALL	ALL	Permit
204.211.38.52/24	UDP	631	Permit
204.211.38.52/24	TCP	25	Deny

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

A. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP.

B. The deny statement for 204 211.38.52/24 should be changed to a permit statement

C. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631

D. The permit statement for 204.211.38 211/24 should be changed to TCP port 631 only instead of ALL

Answer: A

Question #:87 - (Exam Topic 2)

Joe, a contractor, is hired by a firm to perform a penetration test against the firm's infrastructure. While conducting the scan, he receives only the network diagram and the network list to scan against the network. Which of the following scan types is Joe performing?

A. Authenticated

B. White box

C. Automated

D. Gray box

Answer: D

Question #:88 - (Exam Topic 2)

An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL.

B. Implement certificate management.

C. Ensure access to KMS.

D. Use a stronger cipher suite.

Answer: B

Explanation

The **Certificate Management System** (CMS) is a networked **system** for generation, distribution, storage and verification of **certificates** for use in a variety of security enhanced applications. The structure of a **certificate** is defined in the X.509 standard.

Question #:89 - (Exam Topic 2)

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture

B. A user behavior analysis

C. Threat hunting

D. Credentialed vulnerability scanning

Answer: D

Question #:90 - (Exam Topic 2)

A security administrator is Implementing a secure method that allows developers to place files or objects onto a Linux server Developers ate required to log In using a username. password, and asymmetric key. Which of the following protocols should be implemented?

A. SSL/TLS

B. SFTP

C. SRTP

D. IPSec

Answer: B

Question #:91 - (Exam Topic 2)

A security analyst is performing a forensic investigation involving compromised account credentials. Using the Event Viewer, the analyst was able to defect the following message: "Special privileges assigned to new logon.' Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

A. Pass-the-hash

B. Buffer overflow

C. Cross-site scripting

D. Session replay

Answer: B

Question #:92 - (Exam Topic 2)

Which of the following BEST explains the difference between a credentialed scan and a non-credentialed

scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non-credentialed scan sees outward-facing applications.

B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.

C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives

D. A credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.

Answer: D

Question #:93 - (Exam Topic 2)

A technician has been asked to document which services are running on each of a collection of 200 servers. Which of the following tools BEST meets this need while minimizing the work required?

A. Nmap

B. Nslookup

C. Netcat

D. Netstat

Answer: A

Question #:94 - (Exam Topic 2)

A security analyst is investigating a vulnerability In which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?

A. ssh

B. chmod

C. ls

D. setuid

E. nessus

F. nc

Answer: B

Question #:95 - (Exam Topic 2)

A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

```
10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY   FROM:ANY TO:ANY PORT:ANY
```

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following rule to the firewall: 5 PERMIT FROM:ANY TO:ANY PORT:53

B. Replace rule number 10 with the following rule: 10 PERMIT FROM:ANY TO:ANY PORT:22

C. Insert the following rule in the firewall: 25 PERMIT FROM:ANY TO:ANY PORTS:ANY

D. Remove the following rule from the firewall: 30 DENY FROM:ANY TO:ANY PORT:ANY

Answer: B

Question #:96 - (Exam Topic 2)

A company is implementing a tool to mask all PII when moving data from a production server to a testing server. Which of the following security techniques is the company applying?

A. Data wiping

B. Steganograpgy

C. Data obfuscation

D. Data sanitization

Answer: D

Question #:97 - (Exam Topic 2)

A threat actor motivated by political goals that is active for a short period of time but has virtually unlimited resources is BEST categorized as a:

A. hacktivist.

B. nation-state

C. script kiddie

D. APT

Answer: B

Explanation

Nation-State Actors

Actors sponsored by nation-states are characterized by a high level of sophistication and resources. They're capable of carrying out large-scale attacks as well as advanced persistent threats (APTs), which are stealthy attacks whose purpose is to maintain a presence in the network for an extensive period of time, typically to collect targeted types of data. APTs can move laterally through a network and blend in with regular traffic — one of the reasons they can go undetected for months and years and inflict a high degree of damage to an organization.

Nation-state actors focus on several attack vectors simultaneously and exploit a number of vulnerabilities. In recent years, many high-profile attacks have been attributed to nation-state actors.

Some countries use these sophisticated players to fund their regime. But more typically, nation-state actors are not motivated by direct financial gain. Their reasons may lie in national security, political espionage, military intelligence and even attempts to influence another nation's political process. They may also after intellectual property data that could ultimately give the sponsoring nation a competitive advantage on the international market.

This category of attackers is well-funded and operates within an extensive support infrastructure that includes multiple hacker networks. Researchers have also been observing international collaboration between different groups of state-sponsored actors.

Question #:98 - (Exam Topic 2)

Which of the following vulnerabilities can lead to unexpected system behavior, including the bypassing of security controls, due to differences between the time of commitment and the time of execution?

A. Buffer overflow

B. DLL injection

C. Pointer dereference

D. Race condition

Answer: C

Explanation

Buffer overflow protection is any of various techniques used during software development to enhance the security of executable programs by detecting **buffer overflows** on stack-allocated variables, and preventing them from causing program misbehavior or from becoming serious security vulnerabilities.

DLL injection is a technique which **allows an attacker** to run arbitrary code in the context of the address space of another process. If this process **is** running with excessive privileges then it could be abused by an **attacker** in order to execute malicious code in the form of a **DLL** file in order to elevate privileges.

Question #:99 - (Exam Topic 2)

During a security audit of a company's network, unsecure protocols were found to be in use. A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2

B. TLS12

C. SSL13

D. SNMPv3

Answer: A

Explanation

Product and Software: This article applies to all Aruba controllers and ArubaOS versions.

The program Secure Shell (SSH) is a secure replacement for Telnet and the Berkeley r-utilities (rlogin, rsh, rcp, and rdist). SSH provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another. SSH provides strong host-to-host and user authentication as well as secure encrypted communications over an insecure internet.

SSH2 is a more secure, efficient, and portable version of SSH that includes SFTP, which is functionally similar to FTP, but is SSH2 encrypted.

SSH2 key authentication is a feature that Aruba Networks currently does not support and you need to use X509 certificates for authentication. SSH2 private keys can be converted to X509 cert format. Use the same private key to generate a certificate request and have the certificate signed by a valid CA. After the certificate is signed by the CA, it can be uploaded to the controller as 'Public Cert' and used for SSH authentication.

Question #:100 - (Exam Topic 2)

An analyst is concerned about data leaks and wants to restrict access to Internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service Which of the following would be the BEST technology for me analyst to consider implementing?

A. DLP

B. VPC

C. CASB

D. ACL

Answer: A

Question #:101 - (Exam Topic 2)

A technician needs lo document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing

B. Steganography tools

C. Protocol analyzer

D. Wireless scanner

Answer: A

Question #:102 - (Exam Topic 2)

A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

A. Password history

B. Account lockout

C. Account expiration

D. Password complexity

Answer: B

Question #:103 - (Exam Topic 2)

Which of the following algorithms would be used to provide non-repudiation of a file transmission?

A. AES

B. RSA

C. MD5

D. SHA

Answer: C

Explanation

Non-repudiation is the ability to prove that the file uploaded and the file downloaded are identical.

Non-repudiation is an essential part of any secure file transfer solution

End-to-end file non-repudiation is the ability to prove who uploaded a specific file, who downloaded it, and that the file uploaded and the file downloaded are identical. It is a security best practice and required by Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accounta-bility Act (HIPAA), Sarbanes-Oxley Act (SOX), and others.

The ability to provide end-to-end file non-repudiation is an essential part of any secure file transfer solution because it provides the following benefits.

* Guarantees the integrity of the data being transferred

* Plays a valuable forensic role if a dispute arises about the file

* Provides a capability that is required for Guaranteed Delivery

Providing end-to-end file non-repudiation requires using a secure file transfer server that can perform all of the following activities:

* Authenticate each user who uploads or downloads a file

* Check the integrity of each file when uploaded and downloaded

* Compare the server and client-generated integrity check results

* Associate and log the authentication and check results

The cryptographically valid SHA1 and MD5 algorithms are widely used to do file integrity checking. SHA1 is the stronger of these, and is approved for file integrity checking under US Federal Information Processing Standard FIPS 140-2. MOVEit secure file transfer server and MOVEit Automation MFT automation server each have built-in FIPS 140-2 validated cryptographic modules that include the SHA1 and MD5 algorithms, which they use for file integrity checking.

Question #:104 - (Exam Topic 2)

A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?

A. Network access control

B. Configuration manager

C. Application whitelisting

D. File integrity checks

Answer: D

Question #:105 - (Exam Topic 2)

A company recently implemented a new security system. In the course of configuration, the security administrator adds the following entry:

#Whitelist USB\VID_13FE&PID_4127&REV_0100

Which of the following security technologies is MOST likely being configured?

A. Application whitelisting

B. HIDS

C. Data execution prevention

D. Removable media control

Answer: D

Question #:106 - (Exam Topic 2)

A security analyst is specifying requirements for a wireless network. The analyst must explain the security features provided by various architecture choices.

Which of the following is provided by PEAP, EAP-TLS, and EAP-TTLS?

A. Key rotation

B. Mutual authentication

C. Secure hashing

D. Certificate pinning

Answer: B

Question #:107 - (Exam Topic 2)

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege

B. Awareness training

C. Separation of duties

D. Mandatory vacation

Answer: B

Question #:108 - (Exam Topic 2)

A company uses wireless for ail laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?

A. A BPDU guard

B. WPA-EAP

C. IP filtering

D. A WIDS

Answer: D

Question #:109 - (Exam Topic 2)

A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

• www company com (mam website)

• contactus company com (for locating a nearby location)

• quotes company com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com. Which of the following certificate types would BEST meet the requirements?

A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

Answer: B

Question #:110 - (Exam Topic 2)

A buffer overflow can result in:

A. loss of data caused by unauthorized command execution.

B. privilege escalation caused by TPN override.

C. reduced key strength due to salt manipulation.

D. repeated use of one-time keys.

Answer: B

Question #:111 - (Exam Topic 2)

A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was recently involved in a security breach:

<script

src=http://gotcha.com/hackme.js

></script>

Given the line of code above, which of the following BEST represents the attack performed during the breach?

A. CSRF

B. DDoS

C. Dos

D. XSS

Answer: D

Question #:112 - (Exam Topic 2)

A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:

“Your message has been quarantined for the following policy violation: external potential_PII. Please contact the IT security administrator for further details”.

Which of the following BEST describes why this message was received?

A. The DLP system flagged the message.

B. The mail gateway prevented the message from being sent to personal email addresses.

C. The company firewall blocked the recipient’s IP address.

D. The file integrity check failed for the attached files.

Answer: A

Question #:113 - (Exam Topic 2)

Which of the following disaster recovery sites would require the MOST time to get operations beck online?

A. Colocation

B. Cold

C. Hot

D. Warm

Answer: B

Question #:114 - (Exam Topic 2)

An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the Chief Executive Officer (CEO). Which of the following is the best NEXT step for the analyst to take?

A. Call the CEO directly to ensure awareness of the event

B. Run a malware scan on the CEO's workstation

C. Reimage the CEO's workstation

D. Disconnect the CEO's workstation from the network.

Answer: D

Question #:115 - (Exam Topic 2)

A security analyst is emailing PII in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PII data is protected with the following minimum requirements:

*Ensure confidentiality at rest.

* Ensure the integrity of the original email message.

Which of the following controls would ensure these data security requirements are carried out?

A. Encrypt and sign the email using S/MIME.

B. Encrypt the email and send it using TLS.

C. Hash the email using SHA-1.

D. Sign the email using MD5

Answer: A

Question #:116 - (Exam Topic 2)

An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood or an incident, while the horizontal axis indicates the impact.

High	Yellow	Red	Pink
Medium	Green	Yellow	Red
Low	Green	Green	Yellow
	Low	Medium	High

Which of the following is this table an example of?

A. Internal threat assessment

B. Privacy impact assessment

C. Qualitative risk assessment

D. Supply chain assessment

Answer: C

Question #:117 - (Exam Topic 2)

A systems administrator is auditing the company's Active Directory environment. It is quickly noted that the username "company\bsmith" is interactively logged into several desktops across the organization. Which of the following has the systems administrator MOST likely come across?

A. Service account

B. Shared credentials

C. False positive

D. Local account

Answer: B

Question #:118 - (Exam Topic 2)

A security analyst is running a credential-based vulnerability scanner on a Windows host. The vulnerability scanner is using the protocol NetBIOS over TCP/IP to connect to various systems, However, the scan does not return any results. To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135

B. 137

C. 3389

D. 5060

Answer: B

Question #:119 - (Exam Topic 2)

Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

A. Development

B. Staging

C. Production

D. Test

Answer: A

Question #:120 - (Exam Topic 2)

Which of the following control types are alerts sent from a SIEM fulfilling based on vulnerably signatures?

A. Preventive

B. Corrective

C. Compensating

D. Detective

Answer: D

Question #:121 - (Exam Topic 2)

A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Select TWO).

A. 802.1X

B. RADIUS federation

C. WPS

D. Captive portal

E. WPA2

F. WDS

Answer: A E

Question #:122 - (Exam Topic 2)

An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk Is greater than the five-year cost of the insurance policy. The organization is enabling risk:

A. avoidance.

B. acceptance.

C. mitigation.

D. transference.

Answer: B

Question #:123 - (Exam Topic 2)

An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting

B. Clickjacking

C. Buffer overflow

D. Replay

Answer: C

Question #:124 - (Exam Topic 2)

A company has won an important government contract. Several employees have been transferred from their existing projects to support a new contract. Some of the employees who have transferred will be working long hours and still need access to their project information to transition work to their replacements.

Which of the following should be implemented to validate that the appropriate offboarding process has been followed?

A. Separation of duties

B. Time-of-day restrictions

C. Permission auditing

D. Mandatory access control

Answer: C

Question #:125 - (Exam Topic 2)

ON NO: 792

A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step

for the company to take?

A. Consult data disposition policies in the contract.

B. Use a pulper or pulverizer for data destruction.

C. Retain the data for a period no more than one year.

D. Burn hard copies containing PII or PHI

Answer: A

Question #:126 - (Exam Topic 2)

Which of the following are considered to be "something you do"? (Select TWO).

A. Iris scan

B. Handwriting

C. Common Access Card

D. Gait

E. PIN

F. Fingerprint

Answer: B D

Question #:127 - (Exam Topic 2)

While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP

B. SSH

C. SSL

D. DNS

Answer: B

Question #:128 - (Exam Topic 2)

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and Identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement

B. Least privilege

C. An acceptable use policy

D. Off boarding

Answer: B

Question #:129 - (Exam Topic 2)

A security analyst wishes to scan the network to view potentially vulnerable systems the way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan.

B. Conduct an intrusive scan.

C. Attempt escalation of privilege

D. Execute a credentialed scan.

Answer: A

Question #:130 - (Exam Topic 2)

A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was not able to block the malware, but the HIDS alerted to C2 calls as 'Troj.Generic'. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan

B. Spyware

C. Rootkit

D. Botnet

Answer: A

Question #:131 - (Exam Topic 2)

Which of the following provides PFS?

A. AES

B. RC4

C. DHE

D. HMAC

Answer: C

Question #:132 - (Exam Topic 2)

An organization is concerned that Its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -s compwia.org -p 80

B. nc -1 -v compria.org -p 60

C. nmap comptia.org -p 80 -sv

D. nslookup -port-80 compcia.org

Answer: B

Question #:133 - (Exam Topic 2)

After entering a username and password, an administrator must draw a gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

A. Multifactor authentication

B. Something you can do

C. Biometrics

D. Two-factor authentication

Answer: B

Explanation

https://www.androidcentral.com/android-home-screen-gestures

Question #:134 - (Exam Topic 2)

Which of the following is a technical preventive control?

A. Two-factor authentication

B. DVR-supported cameras

C. Acceptable-use MOTD

D. Syslog server

Answer: A

Question #:135 - (Exam Topic 2)

NO: 906

A user receives a security alert pop-up from the host-based IDS, and a few minutes later notices a document on the desktop has disappeared and in its place is an odd filename with no icon image. When clicking on this icon, the user receives a system notification that it cannot find the correct program to use to open this file. Which of the following types of malware has MOST likely targeted this workstation?

A. Rootkit

B. Spyware

C. Ransomware

D. Remote-access Trojan

Answer: C

Question #:136 - (Exam Topic 2)

A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator. Which of the following protocols should be configured on the RADIUS server? (Select TWO).

A. PAP

B. MSCHAP

C. PEAP

D. NTLM

E. SAML

Answer: B C

Question #:137 - (Exam Topic 2)

A small enterprise decides to implement a warm site to be available for business continuity in case of a disaster. Which of the following BEST meets its requirements?

A. A fully operational site that has all the equipment in place and full data backup tapes on site

B. A site used for its data backup storage that houses a full-time network administrator

C. An operational site requiring some equipment to be relocated as well as data transfer to the site

D. A site staffed with personnel requiring both equipment and data to be relocated there in case of disaster

Answer: C

Explanation

Cold site

Space and associated infrastructure (e.g., power, telecoms and environmental controls to support IT systems), which will only be installed when disaster recovery (DR) services are activated.

Warm site

Site that's partially equipped with some of the equipment (e.g., computing hardware and software, and supporting personnel); organizations install additional equipment, computing hardware and software, and supporting personnel when DR services are activated.

Hot site

Fully equipped site with the required equipment, computing hardware/software and supporting personnel; it's also fully functional and manned on a 24x7 basis so that it's ready for organizations to operate their IT systems when DR services are activated.

Question #:138 - (Exam Topic 2)

Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.

B. The test Is performed against the wrong host.

C. The signature matches the product but not the version information.

D. The hosts are evaluated based on an OS-specific profile.

Answer: C

Question #:139 - (Exam Topic 2)

An organization with a low tolerance tor user inconvenience wants to protect laptop hard drives against loss of data theft Which of the following would be the MOST acceptable?

A. SED

B. HSU

C. DLP

D. TPM

Answer: C

Question #:140 - (Exam Topic 2)

A company has just completed a vulnerability scan of its servers. A legacy application that monitors the HVAC system in the datacenter presents several challenges, as the application vendor is no longer in business.

Which of the following secure network architecture concepts would BEST protect the other company servers if the legacy server were to be exploited?

A. Virtualization

B. Air gap

C. VLAN

D. Extranet

Answer: B

Question #:141 - (Exam Topic 2)

An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network.

B. Review firewall and IDS logs to identify possible source IPs.

C. Identify and apply any missing operating system and software patches.

D. Delete the malicious software and determine if the servers must be reimaged.

Answer: A

Explanation

Now, since the organization top priority is more of containment over eradication, an outbreak code that is hostile as a can be suppressed effectively by removing the web server completely from the overall network facilities or infrastructure. Also, if the affected servers are not removed, it might affect the integrity, confidentiality of sensitive materials or documents which will be exposed to the outside world by the attacker.

Read more on Brainly.com - https://brainly.com/question/16835492#readmore

Question #:142 - (Exam Topic 2)

Which of the following are the BEST selection criteria to use when assessing hard drive suitability for time-sensitive applications that deal with large amounts of critical information? (Select TWO).

A. MTBF

B. MTTR

C. SLA

D. RTO

E. MTTF

F. RPO

Answer: A B

Question #:143 - (Exam Topic 2)

An organization is struggling to differentiate threats from normal traffic and access to systems A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in Identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?

A. Web application firewall

B. SIEM

C. IPS

D. UTM

E. File integrity monitor

Answer: B

Question #:144 - (Exam Topic 2)

Which of the following are considered among the BEST indicators that a received message is a hoax? (Choose two.)

A. Minimal use of uppercase letters in the message

B. Warnings of monetary loss to the receiver

C. No valid digital signature from a known security organization

D. Claims of possible damage to computer hardware

E. Embedded URLs

Answer: C E

Question #:145 - (Exam Topic 2)

A systems administrator is implementing a remote access method for the system that will utilize GUI. Which of the following protocols would be BEST suited for this?

A. TLS

B. SSH

C. SFTP

D. SRTP

Answer: B

Question #:146 - (Exam Topic 2)

Which of !he following Impacts are associated with vulnerabilities in embedded systems? (Select TWO).

A. Repeated exploitation due to unpatchtable firmware

B. Denial of service due to an integrated legacy operating system

C. Loss of inventory accountability due to device deployment

D. Key reuse and collision Issues due to decentralized management

E. Exhaustion of network resources resulting from poor NIC management

Answer: A B

Question #:147 - (Exam Topic 2)

A government contracting company Issues smartphones lo employees lo enable access lo corporate resources. Several employees will need to travel to a foreign country (or business purposes and will require access lo their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the risk of compromise while on foreign soil?

A. Disable firmware OTA updates.

B. Disable location services.

C. Disable push notification services.

D. Disable wipe.

Answer: A

Question #:148 - (Exam Topic 2)

Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP

B. Public and private keys

C. HOTP token and logon credentials

D. Source and destination IP addresses

Answer: A

Explanation

What is the process for logging in?

Setting up two-factor authentication for a user for the first time:

1. A user will go to the URL given to them by OT support and enter their username and password.

2. After logging in, they'll be prompted to input their phone number and verify it with a simple phone call or text message.

3. The next step is to install Duo Mobile, a smartphone app that generates passcodes and supports Duo Push (on iPhone and Android).

4. After installing the app, it needs to be activated in order to be linked to the user's account.

5. Lastly, the user is shown a success message and the login prompt that they'll normally see when logging in.

To connect via VPN using two-factor authentication after set-up:

Go to the URL and login with their username and password.

1. Choose which authentication method: Duo Push, phone call, text or passcode.

2. If they choose Duo Push, a notification will be sent to their phone. They simply have to select the "Approve" button to redirect their browser to the SSL VPN ser-vice homepage.

3. Then they can launch "Tunnel Mode" to direct traffic through their VPN.

4. See What are the authentication choices? for more information on how each method works.

Question #:149 - (Exam Topic 2)

Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone

B. To capture packets sent to a honeypot during an attack

C. To protect hard disks from access during a forensics investigation

D. To restrict access to a building allowing only one person to enter at a time

Answer: A

Question #:150 - (Exam Topic 2)

Users are attempting to access a company's website but are transparently redirected to another websites. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC

B. HTTPS

C. IPSec

D. TLS/SSL

Answer: A

Question #:151 - (Exam Topic 2)

A network technician needs to monitor and view the websites that are visited by an employee. The employee Is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?

A. Implement promiscuous mode on the NIC of the employee's computer.

B. Install and configure a transparent proxy server.

C. Run a vulnerability scanner to capture DNS packets on the router.

D. Configure a VPN to forward packets to the technician's computer.

Answer: B

Question #:152 - (Exam Topic 2)

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0

B. 1

C. 5

D. 6

Answer: B

Question #:153 - (Exam Topic 2)

Which of the following would provide a safe environment for an application to access only the resources needed to function while not having access to run at the system level?

A. Sandbox

B. Honey pot

C. GPO

D. DMZ

Answer: A

Question #:154 - (Exam Topic 2)

Which of the following is an example of resource exhaustion?

A. A penetration tester requests every available IP address from a DHCP server.

B. A SQL injection attack returns confidential data back to the browser.

C. Server CPU utilization peaks at 100% during the reboot process

D. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.

Answer: A

Question #:155 - (Exam Topic 2)

A large Industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall whitelisting

C. Containment

D. Isolation

Answer: B

Question #:156 - (Exam Topic 2)

The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat

B. Social engineering

C. Passive reconnaissance

D. Phishing

Answer: B

Question #:157 - (Exam Topic 2)

Two companies are enabling TLS on their respective email gateways to secure communications over the Internet. Which of the following cryptography concepts is being implemented?

A. Perfect forward secrecy

B. Ephemeral keys

C. Domain validation

D. Data in transit

Answer: D

Question #:158 - (Exam Topic 2)

An organization's research department uses workstations in an air-gapped network. A competitor released products based on files that originated in the research department. Which of the following should management do to improve the security and confidentiality of the research files?

A. Implement multifactor authentication on the workstations.

B. Configure removable media controls on the workstations.

C. Install a web application firewall in the research department.

D. Install HIDS on each of the research workstations.

Answer: B

Topic 3, Simulations

Question #:1 - (Exam Topic 3)

An attack has occurred against a company.

INSTRUCTIONS

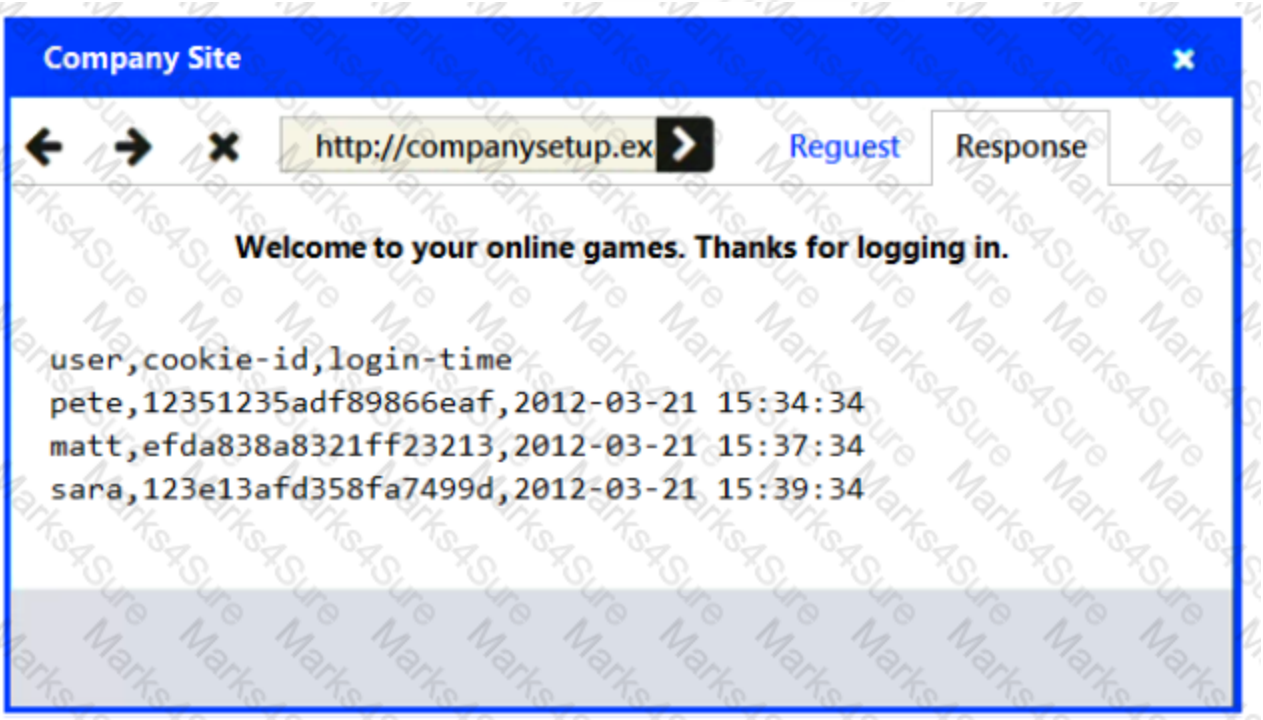
You have been tasked to do the following:

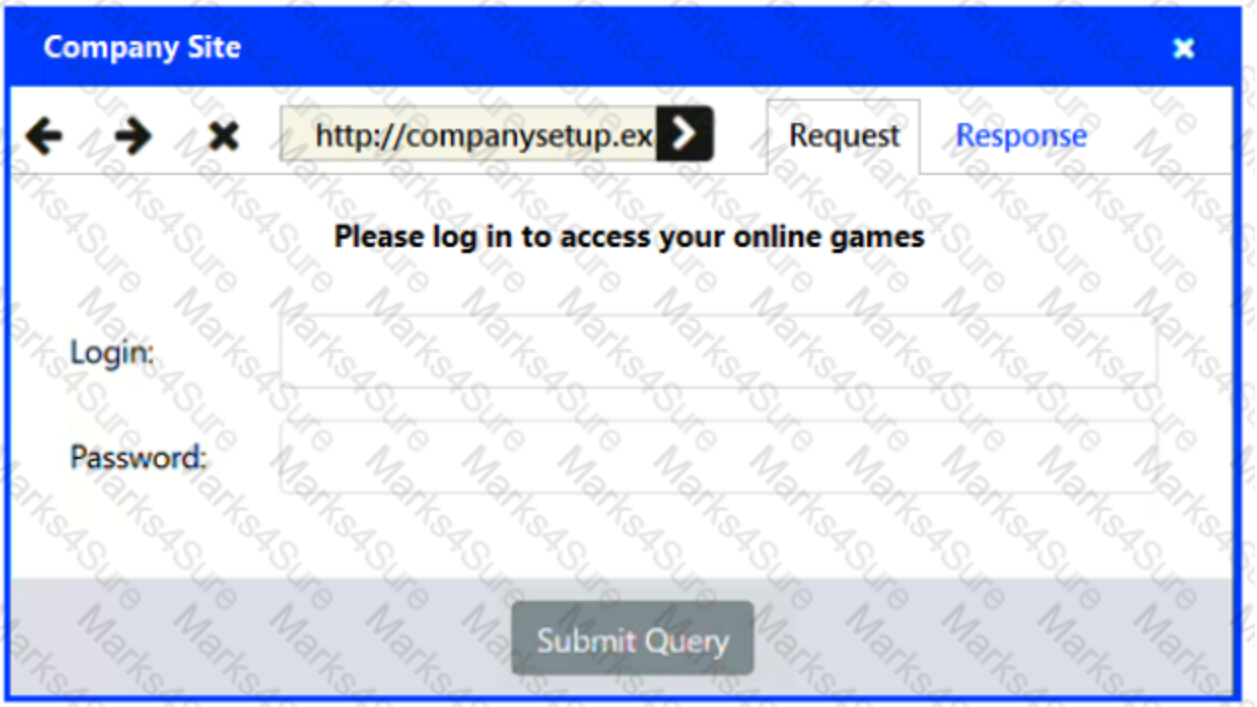
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1)

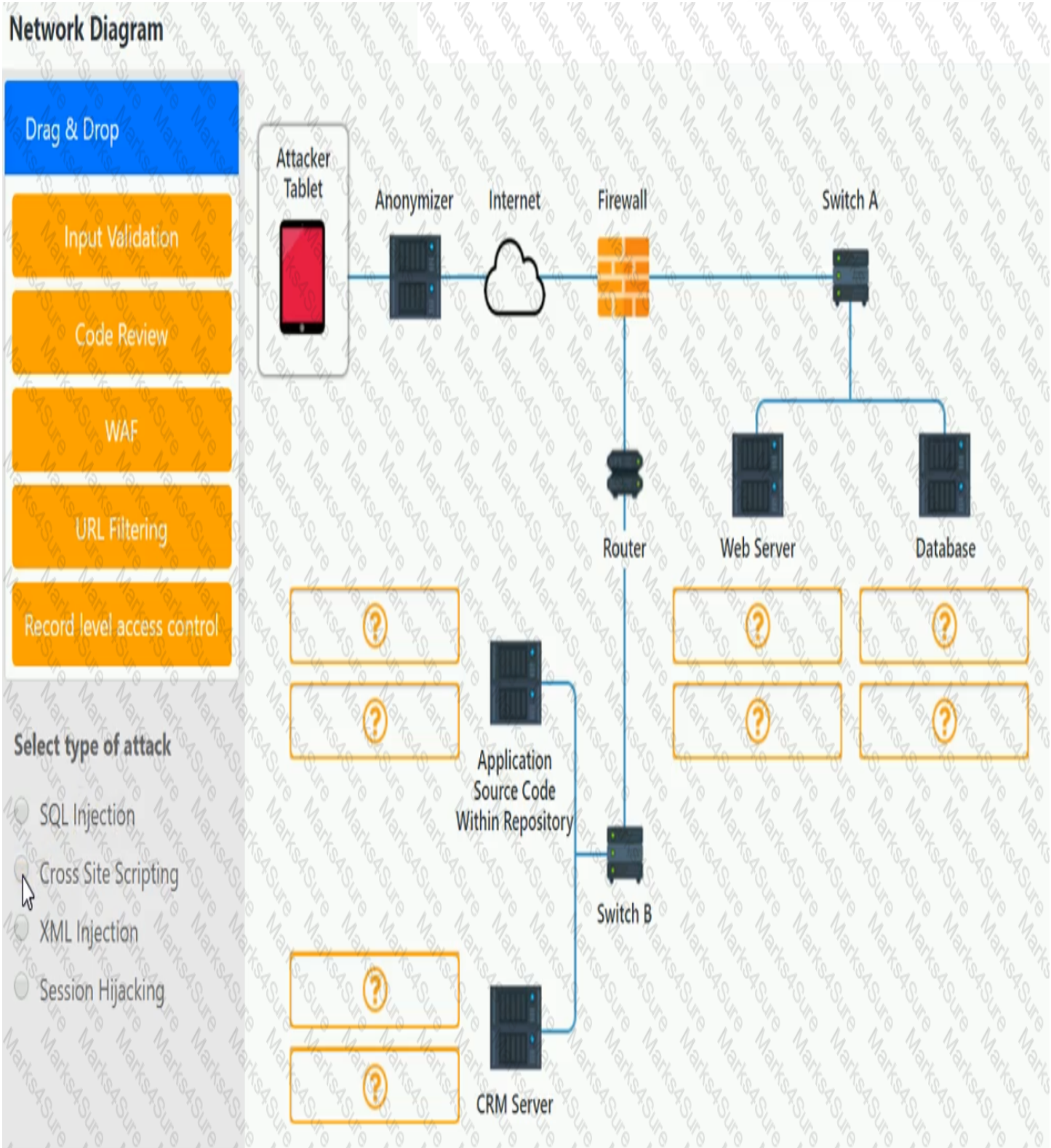
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server. (Answer area 2)

All objects will be used, but not all placeholders may be filled. Objects may only be used once.

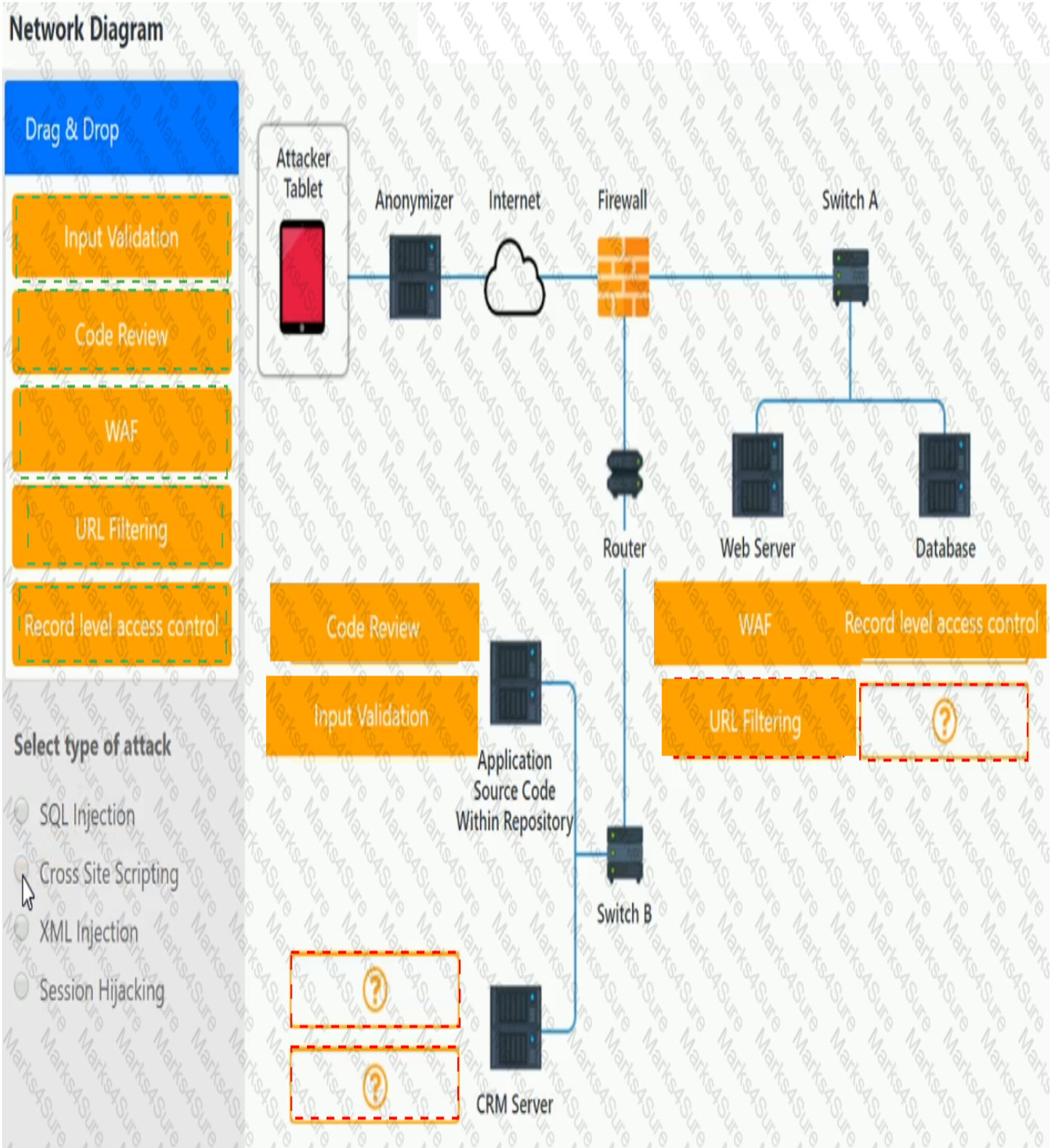
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



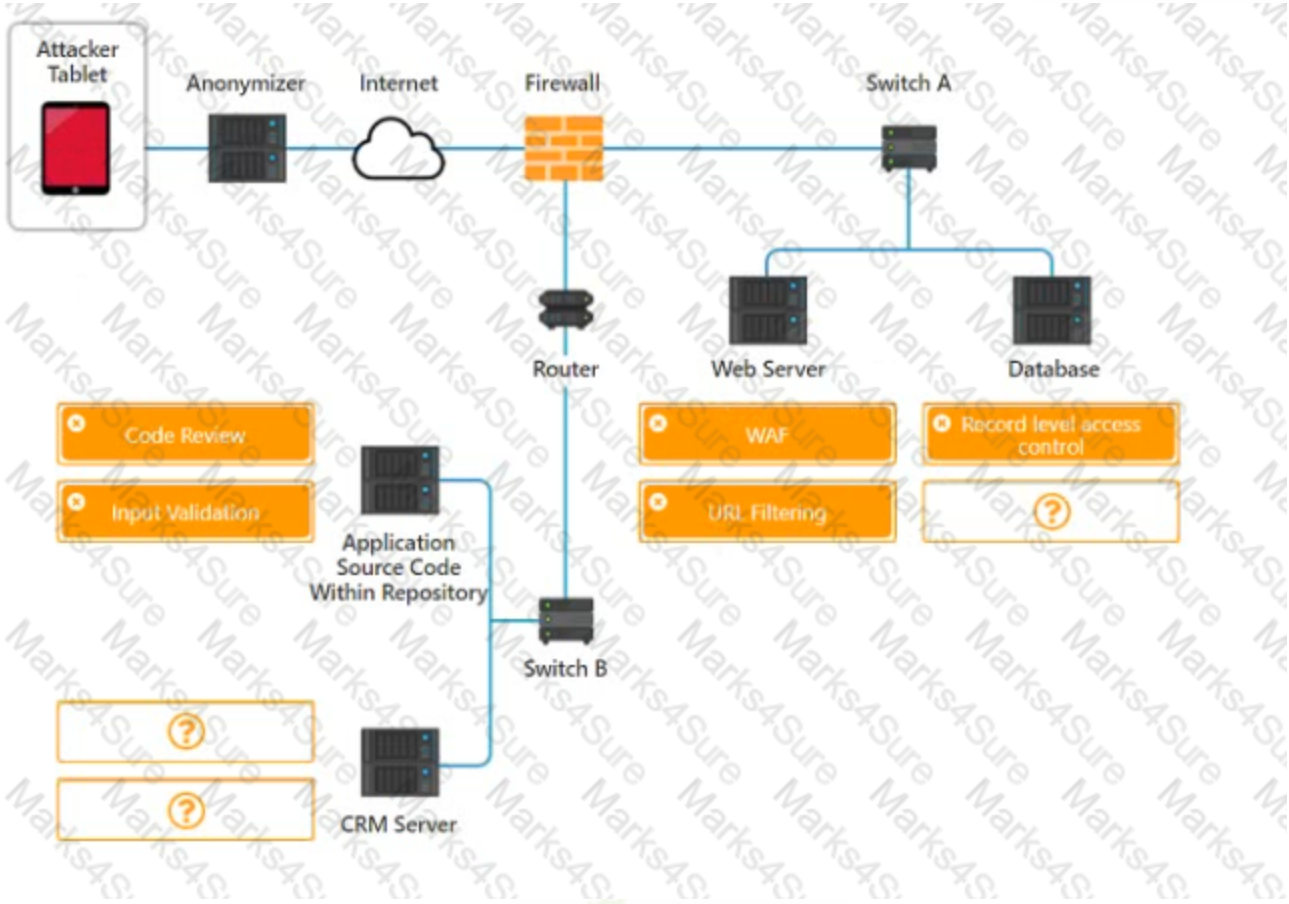

Company Site
http://companysetup.ex
Request
Response
Please log in to access your online games
Login:
Password:
Submit Query

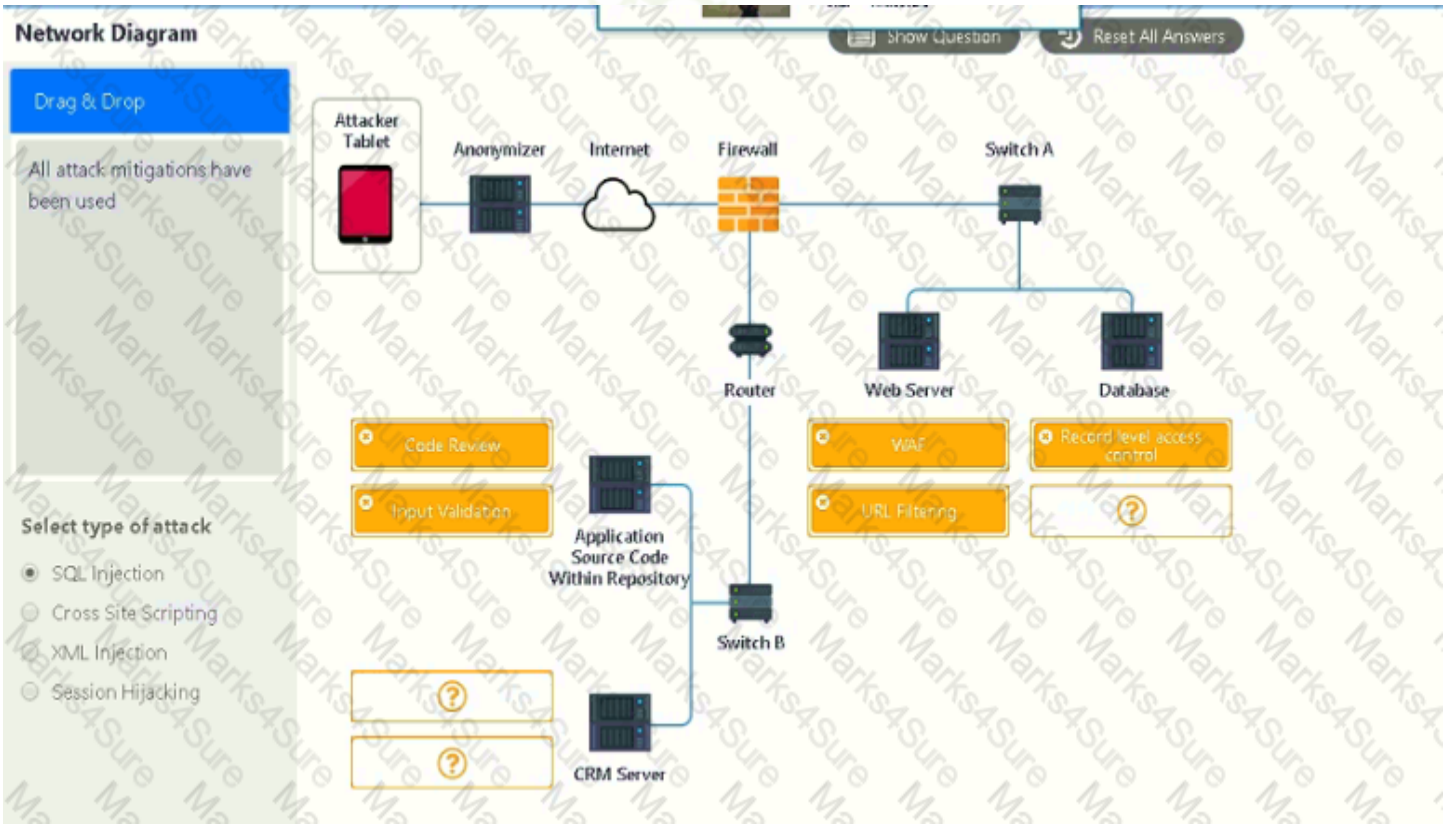

Network Diagram
Drag & Drop
Input Validation
Code Review
WAF
URL Filtering
Record level access control
Select type of attack
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Application Source Code Within Repository
Switch B
CRM Server

Answer:



Explanation


Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Code Review
Input Validation
Application Source Code Within Repository
WAF
URL Filtering
Record level access control
Switch B
CRM Server


Network Diagram
Show Question
Reset All Answers
Drag & Drop
All attack mitigations have been used
Select type of attack
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Code Review
Input Validation
Application Source Code Within Repository
WAF
URL Filtering
Record level access control
Switch B
CRM Server

Question #:2 - (Exam Topic 3)

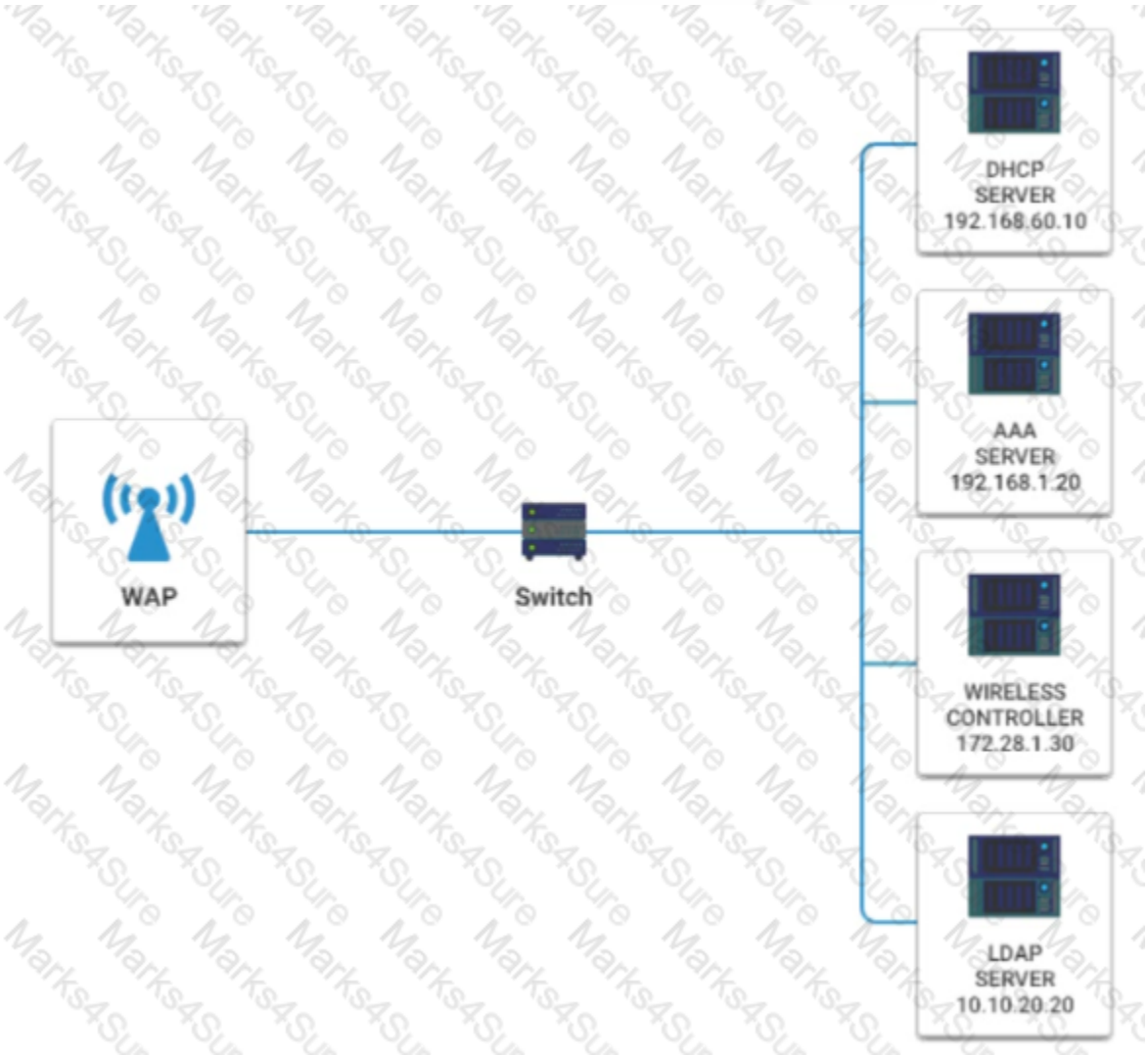
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

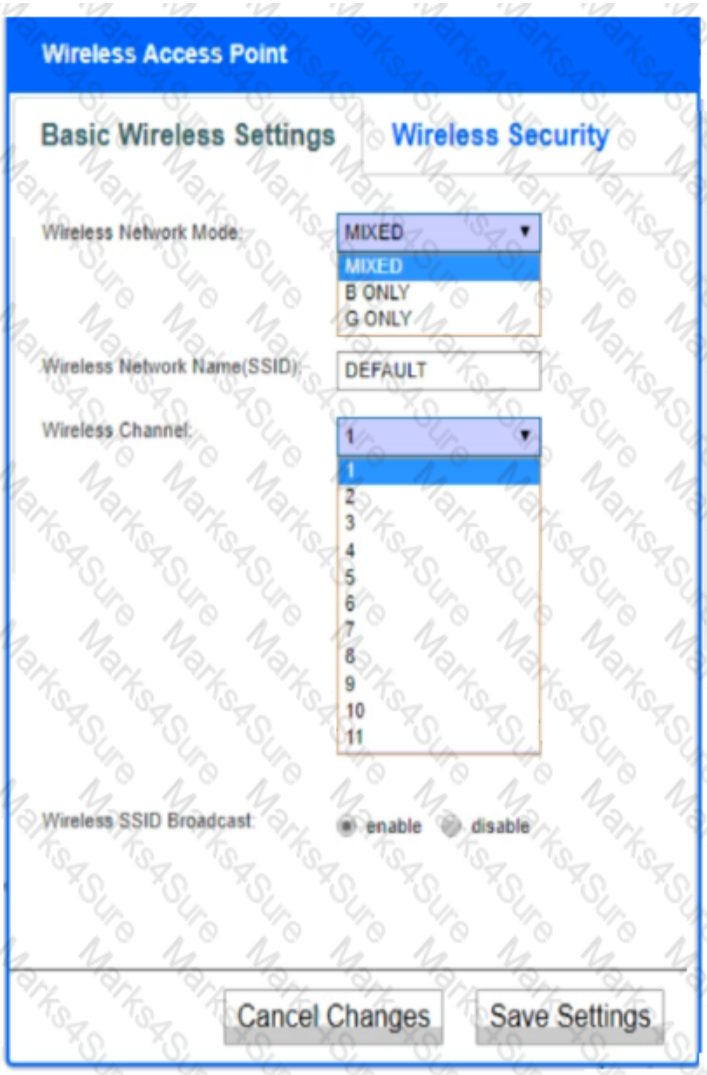
INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:

- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server

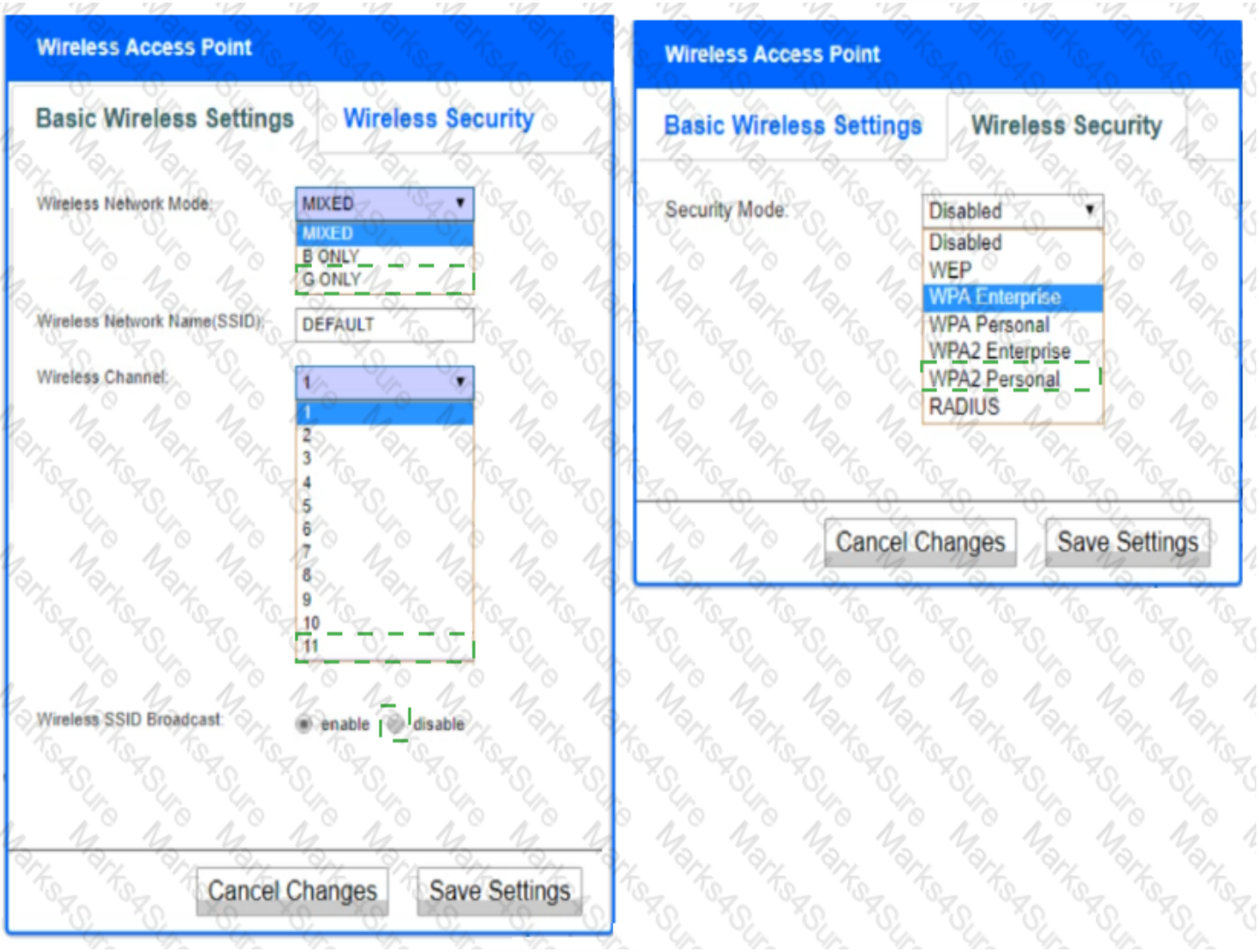
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.




Wireless Access Point
Basic Wireless Settings
Wireless Security
Wireless Network Mode:
MIXED
MIXED
B ONLY
G ONLY
Wireless Network Name(SSID):
DEFAULT
Wireless Channel:
1
1
2
3
4
5
6
7
8
9
10
11
Wireless SSID Broadcast:
enable
disable
Cancel Changes
Save Settings


Wireless Access Point
Basic Wireless Settings
Wireless Security
Security Mode:
Disabled
Disabled
WEP
WPA Enterprise
WPA Personal
WPA2 Enterprise
WPA2 Personal
RADIUS
Cancel Changes
Save Settings

Answer:



Explanation

Wireless Access Point

Network Mode – G only

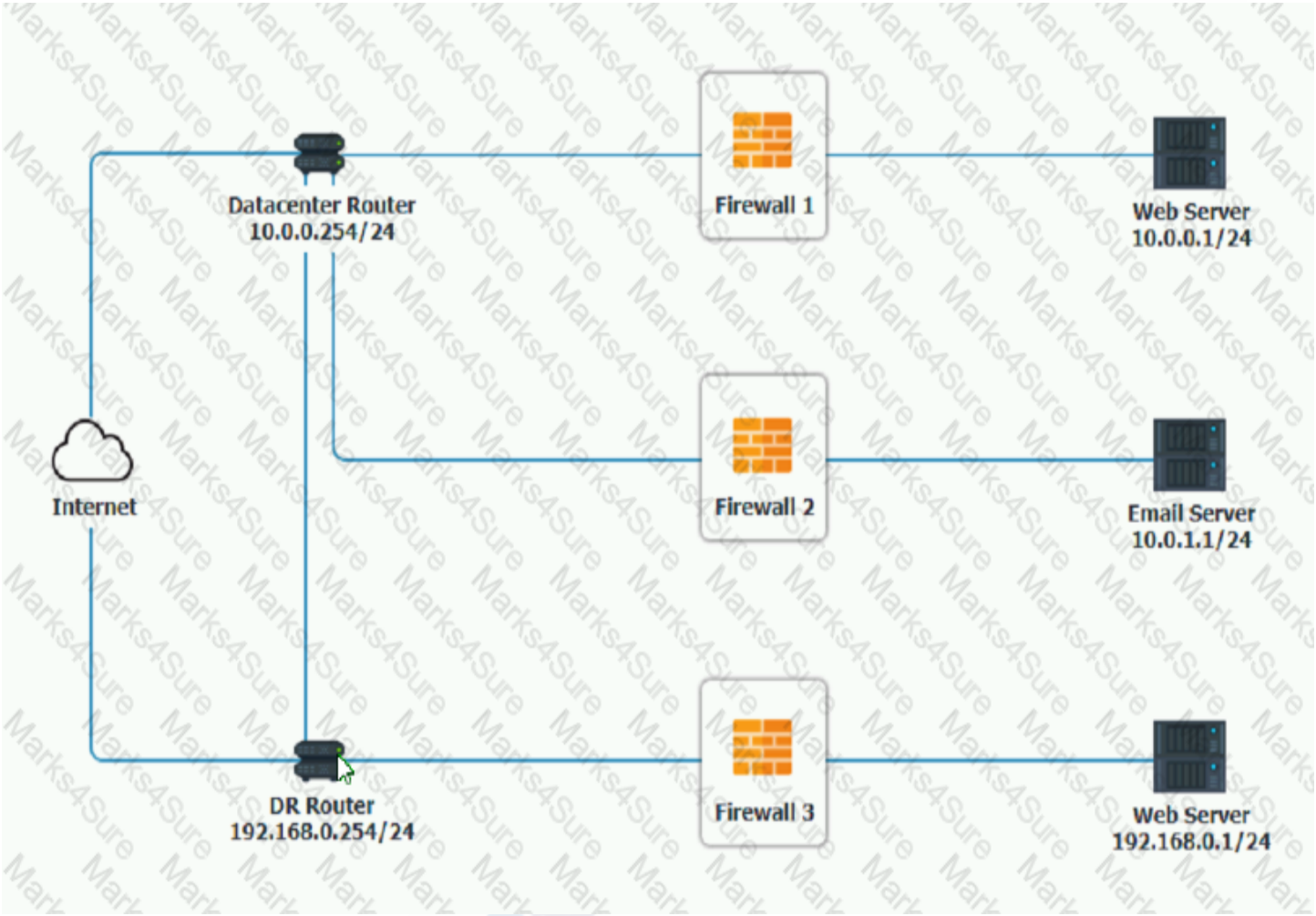
Wireless Channel – 11

Wireless SSID Broadcast – disable

Security settings – WPA2 Professional

Question #:3 - (Exam Topic 3)

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.



INSTRUCTIONS

Click on each firewall to do the following:

1. Deny cleartext web traffic

2. Ensure secure management protocols are used.

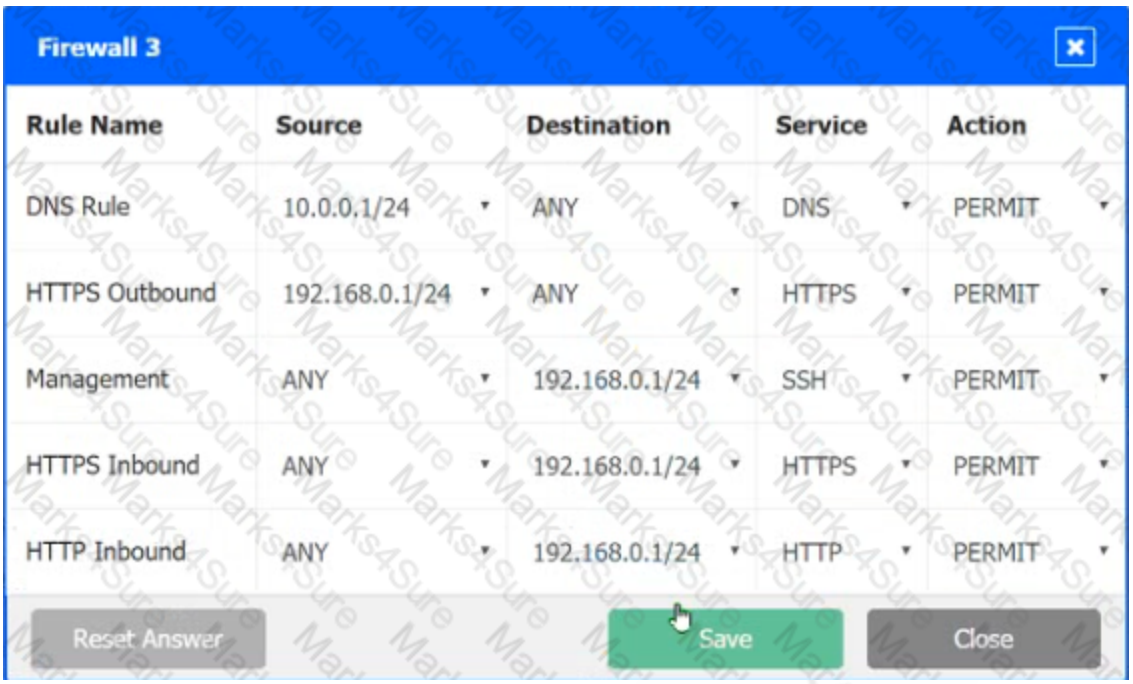
3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.


Firewall 1
Rule Name
Source
Destination
Service
Action
DNS Rule
10.0.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
10.0.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
10.0.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
10.0.0.1/24
HTTPS
PERMIT
HTTP Inbound
ANY
10.0.0.1/24
HTTP
PERMIT
Reset Answer
Save
Close


Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
10.0.1.1/24
ANY
DNS
PERMIT
HTTPS Outbound
10.0.1.1/24
ANY
HTTPS
PERMIT
Management
ANY
10.0.1.1/24
TELNET
PERMIT
HTTPS Inbound
ANY
10.0.1.1/24
HTTPS
PERMIT
HTTP Inbound
ANY
10.0.1.1/24
HTTP
DENY
Reset Answer
Save
Close

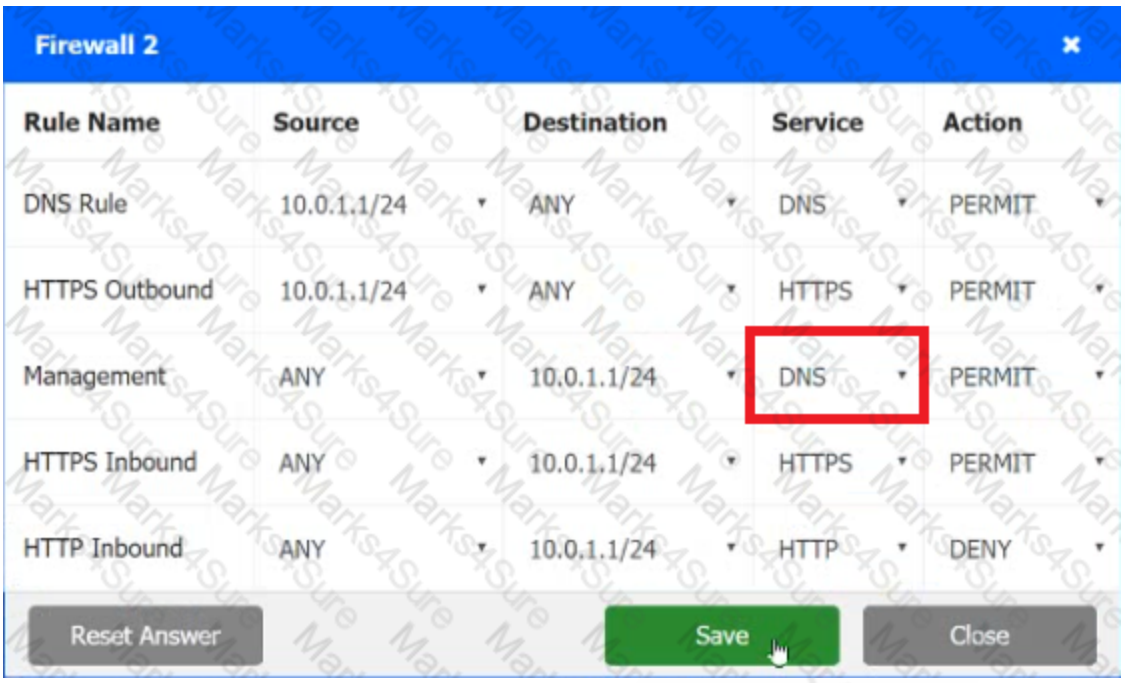


Check the answer in explanation.

Explanation

In Firewall 1, HTTP inbound Action should be DENY. As shown below

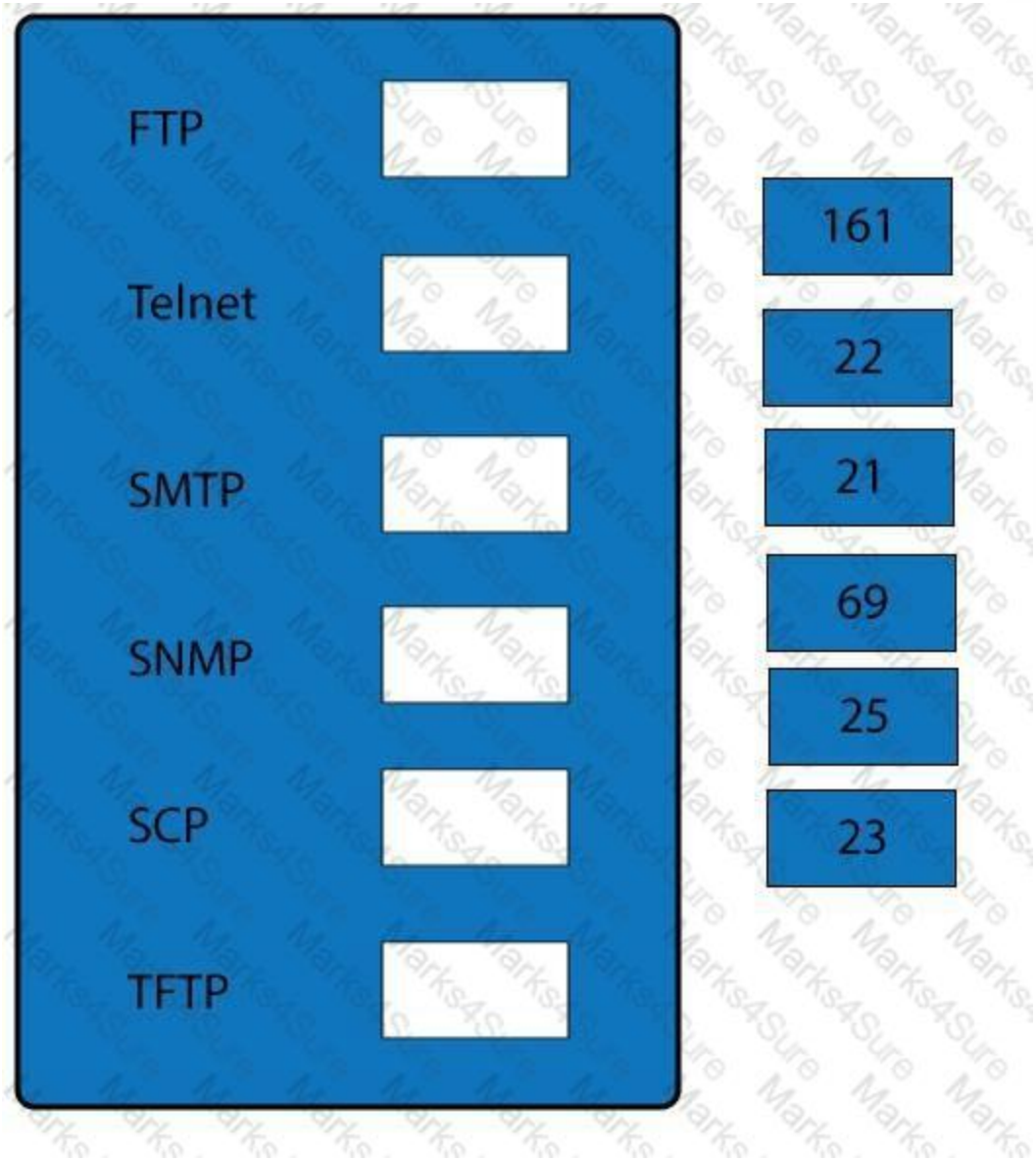
In Firewall 2, Management Service should be **DNS**, As shown below.



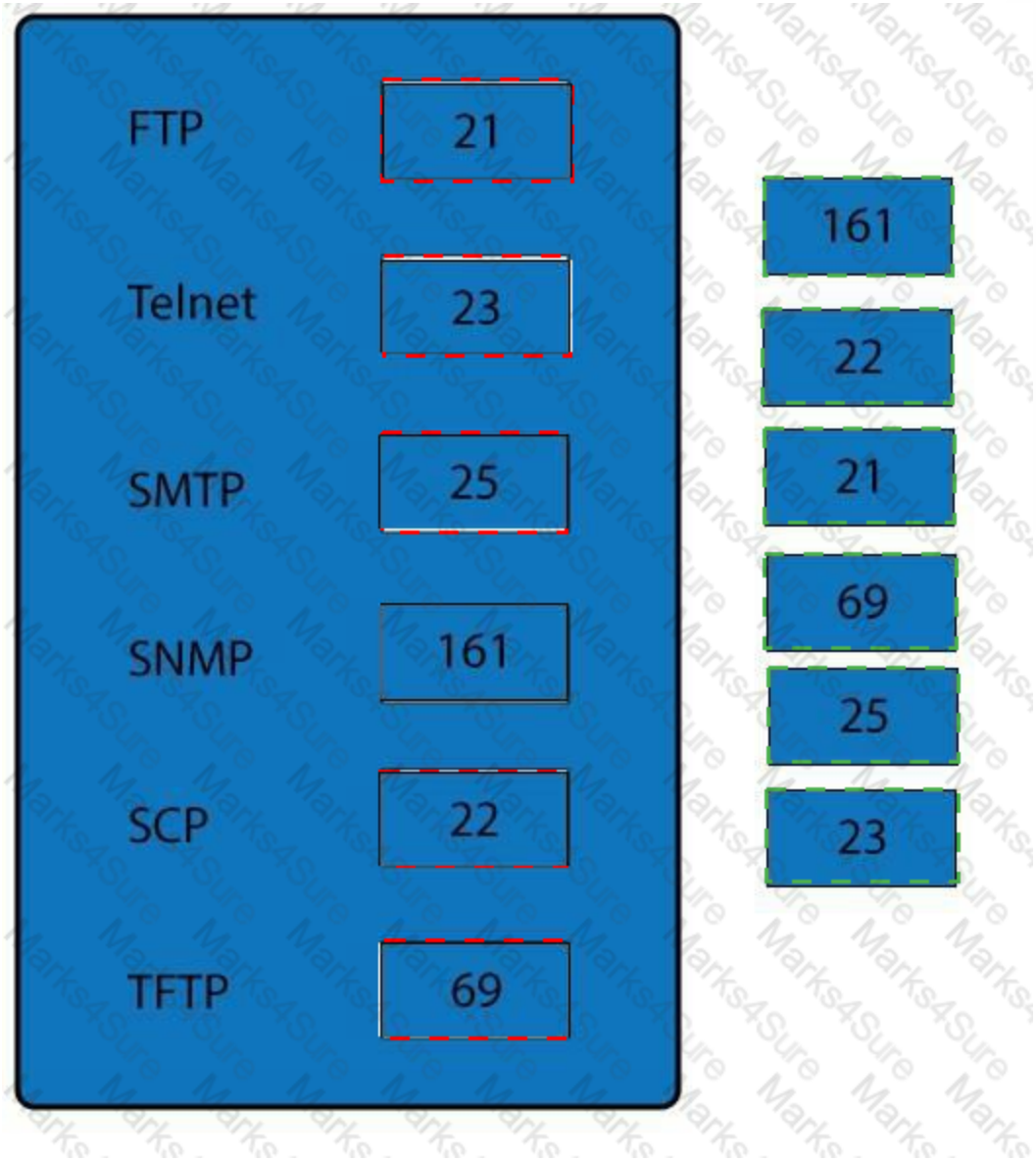
In Firewall 3, HTTP Inbound Action should be DENY, as shown below

Question #:4 - (Exam Topic 3)

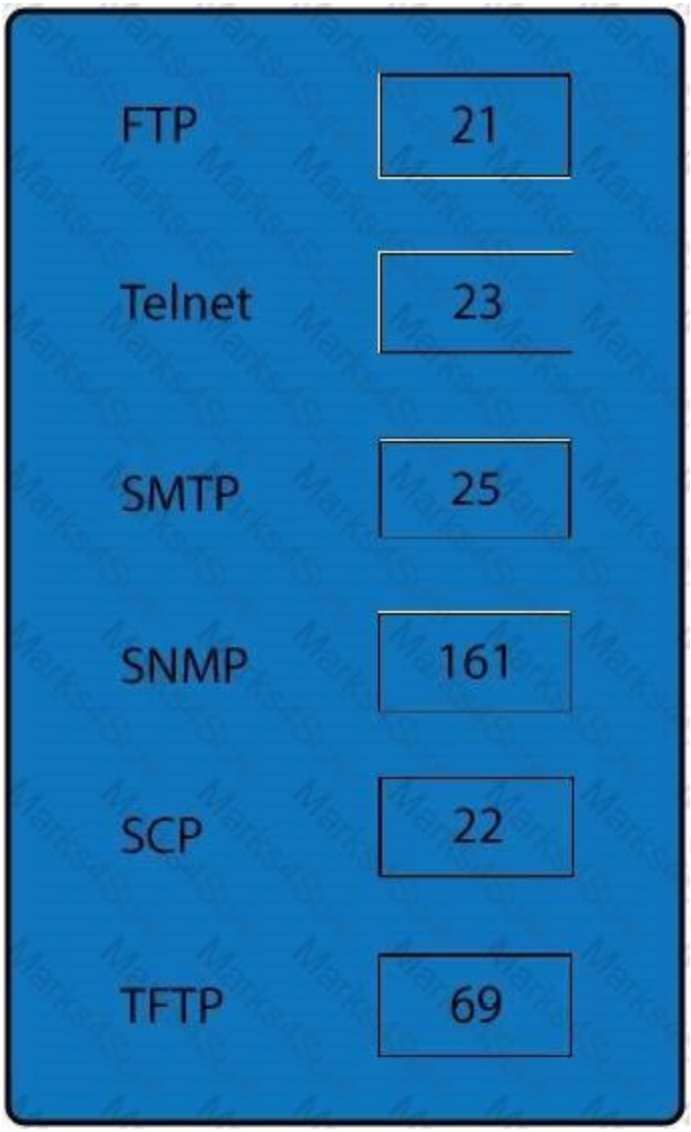
Drag and drop the correct protocol to its default port.



Answer:



Explanation



FTP uses TCP port 21. Telnet uses port 23.

SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP

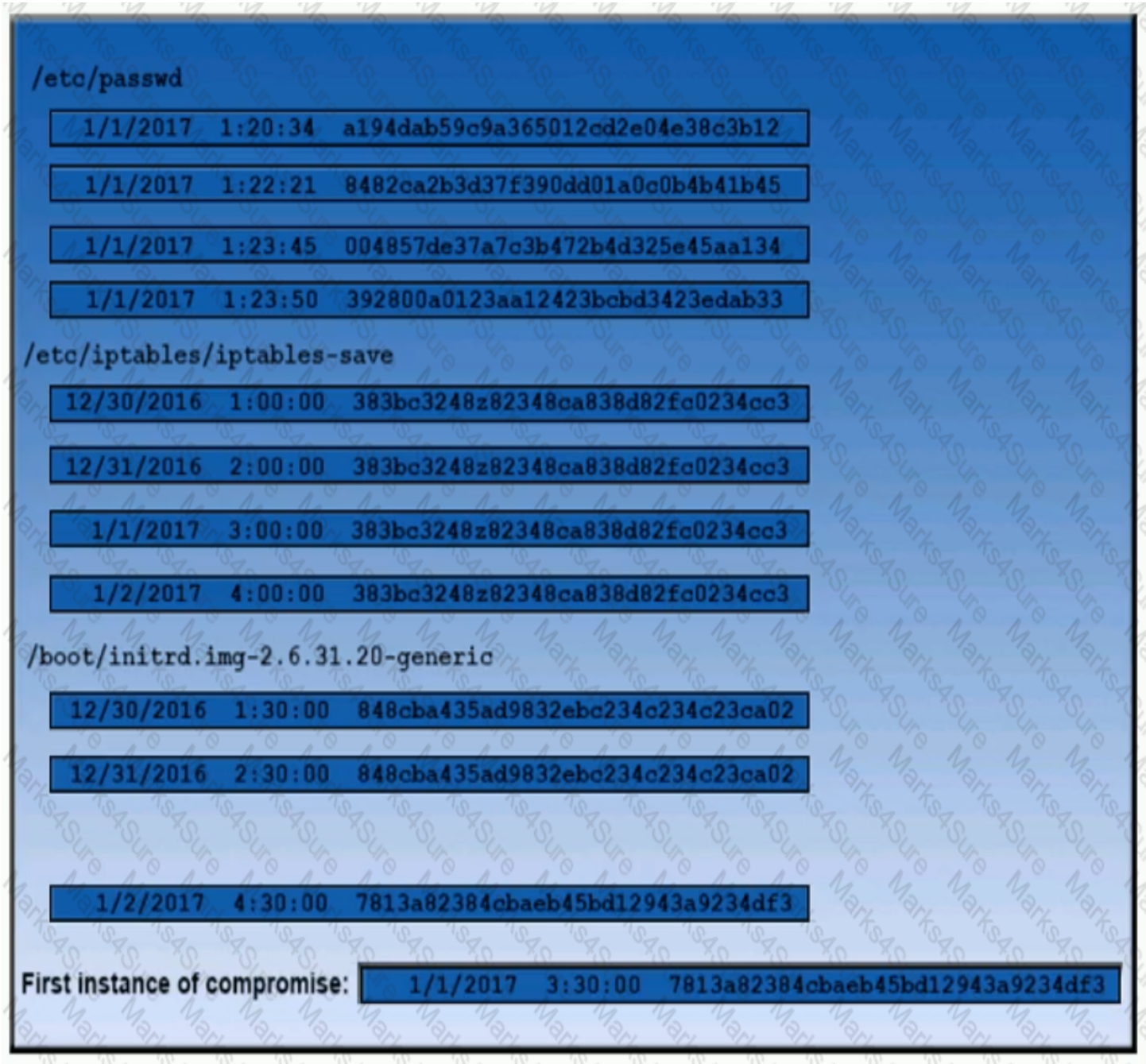
makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question #:5 - (Exam Topic 3)

A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

Answer:

Explanation



Question #:6 - (Exam Topic 3)

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

Answer:

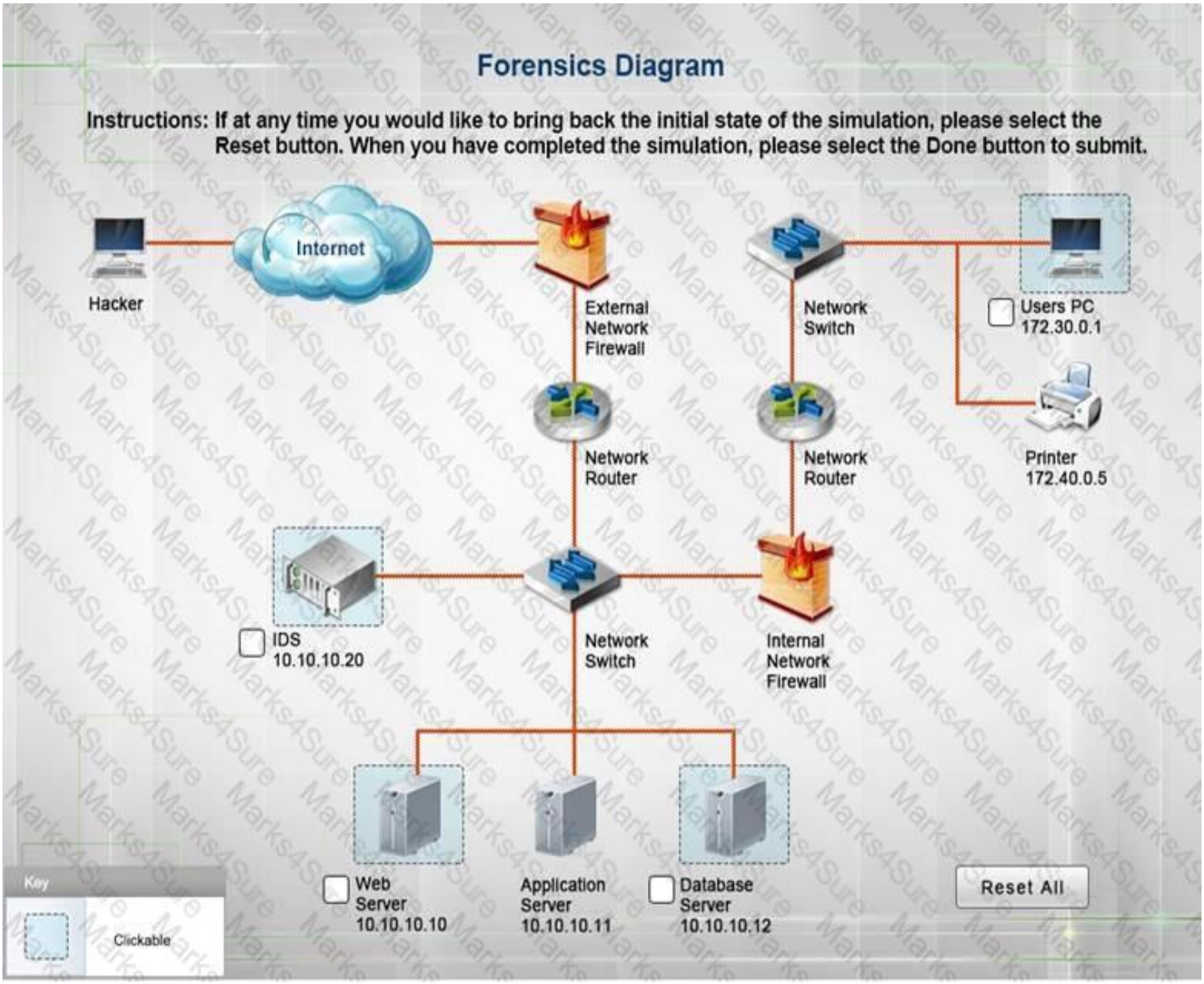
Explanation

Question #:7 - (Exam Topic 3)

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.

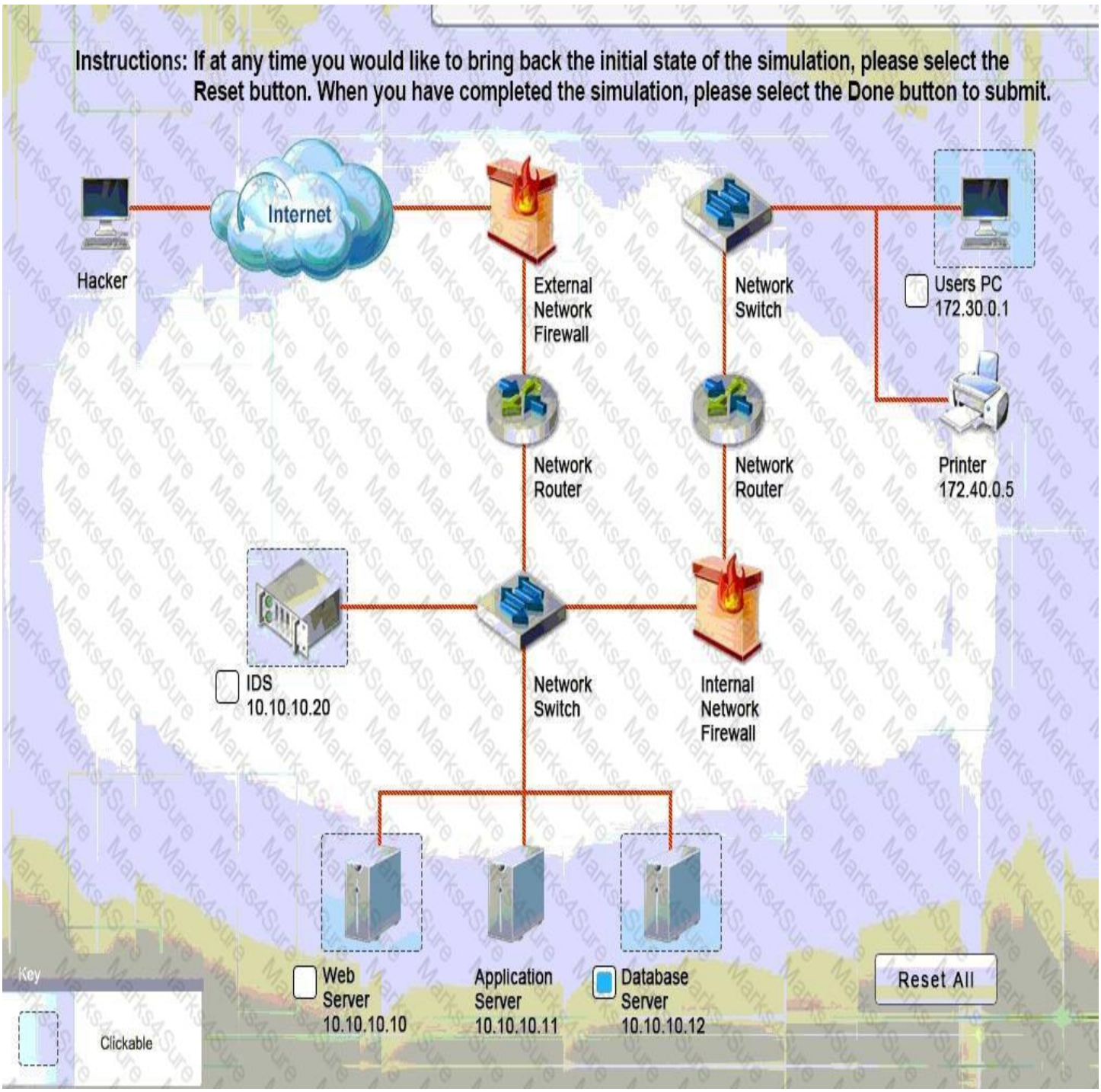
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset 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.



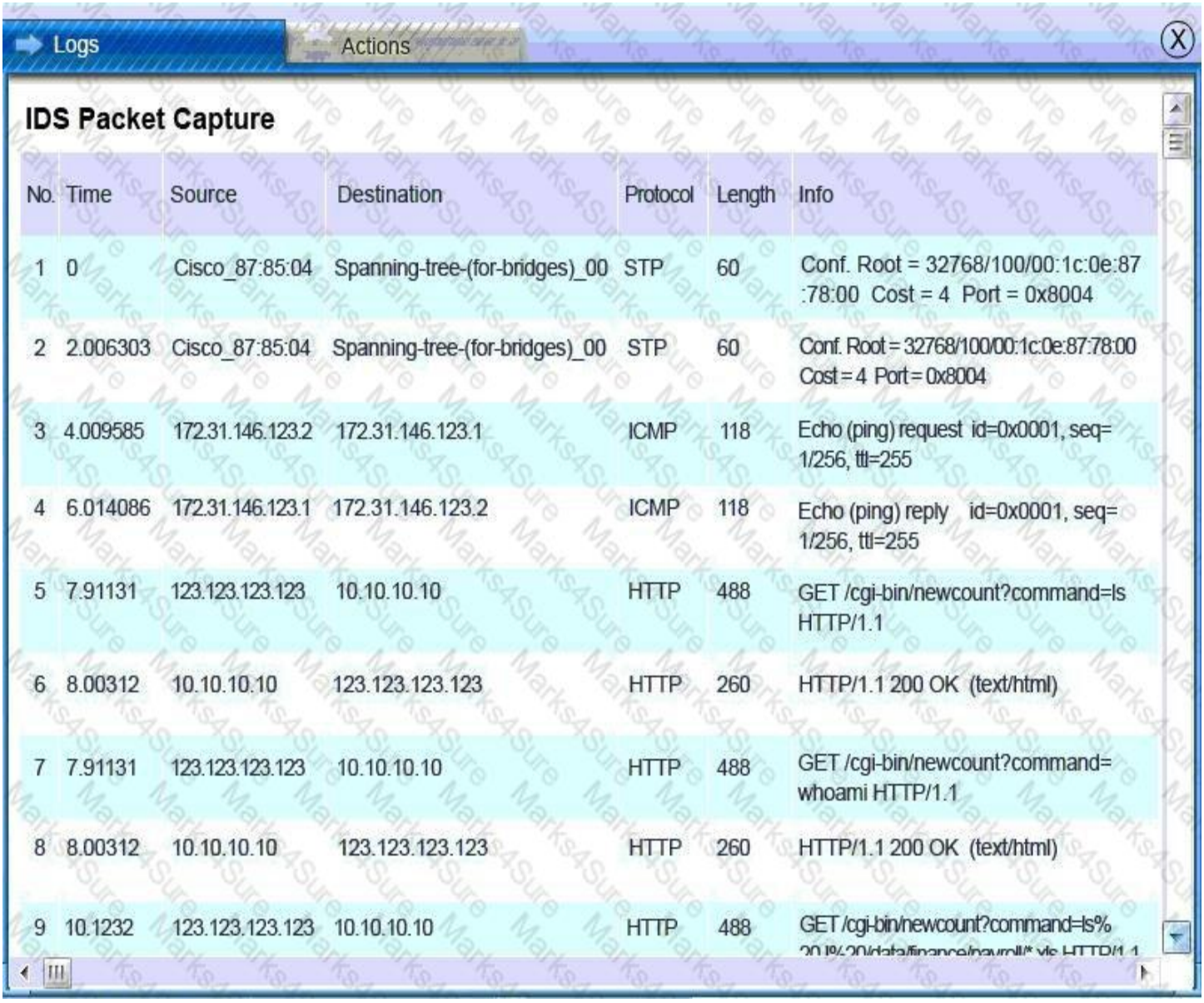
See the solution below.

Explanation

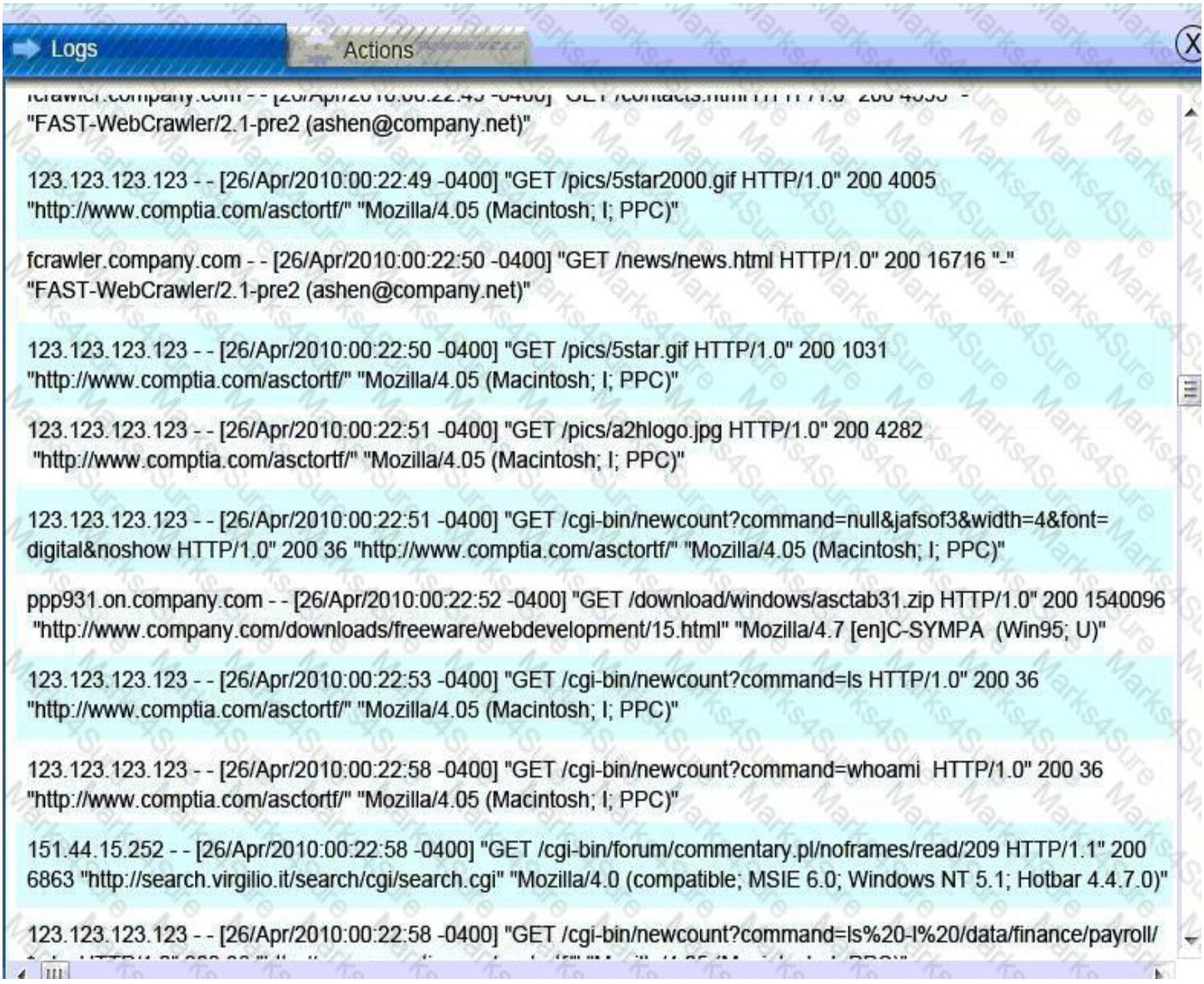
Database server was attacked, actions should be to capture network traffic and Chain of Custody.

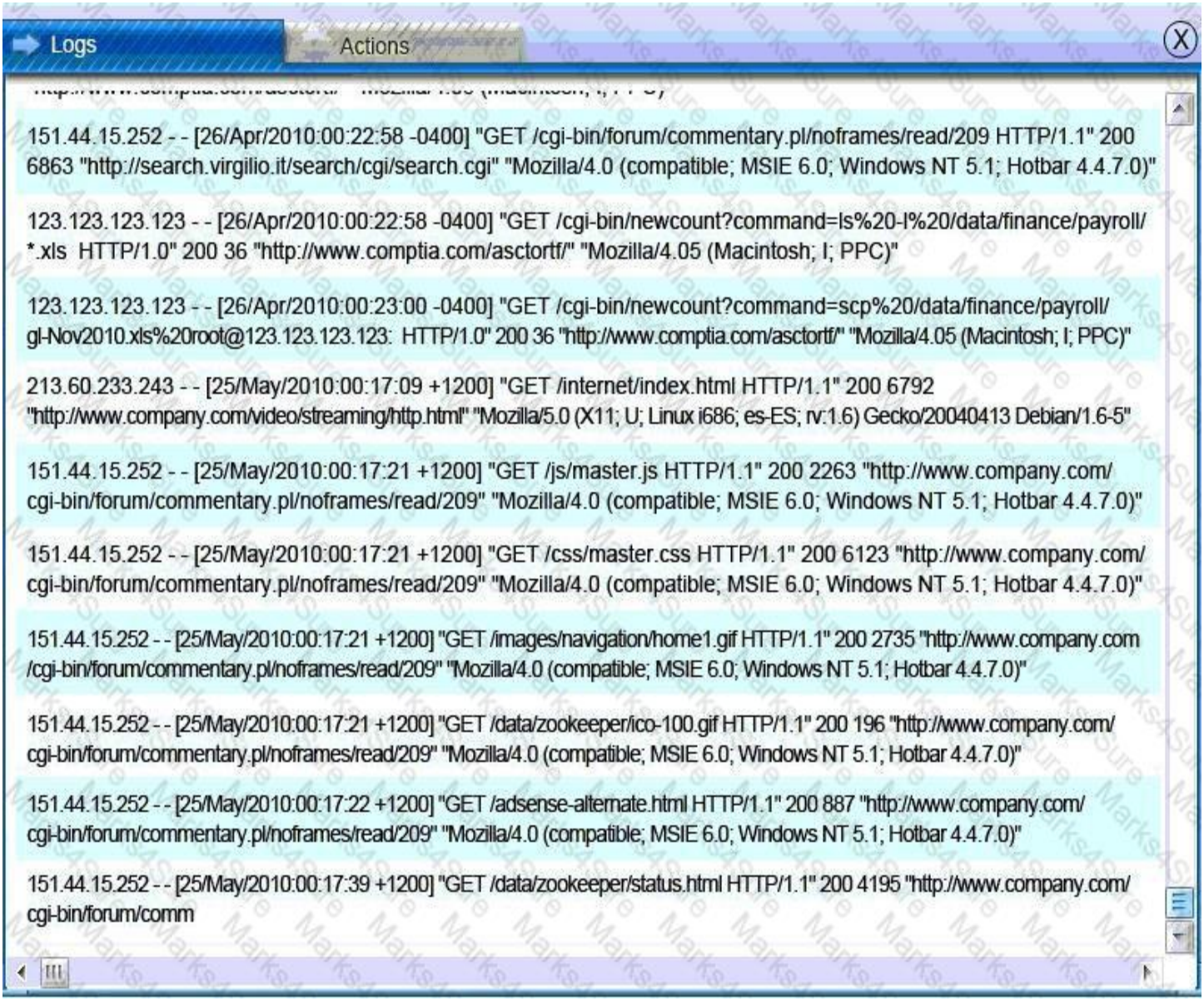

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.
Internet
Hacker
External Network Firewall
Network Switch
Users PC 172.30.0.1
Network Router
Network Router
Printer 172.40.0.5
IDS 10.10.10.20
Network Switch
Internal Network Firewall
Web Server 10.10.10.10
Application Server 10.10.10.11
Database Server 10.10.10.12
Reset All
Key
Clickable

IDS Server Log:

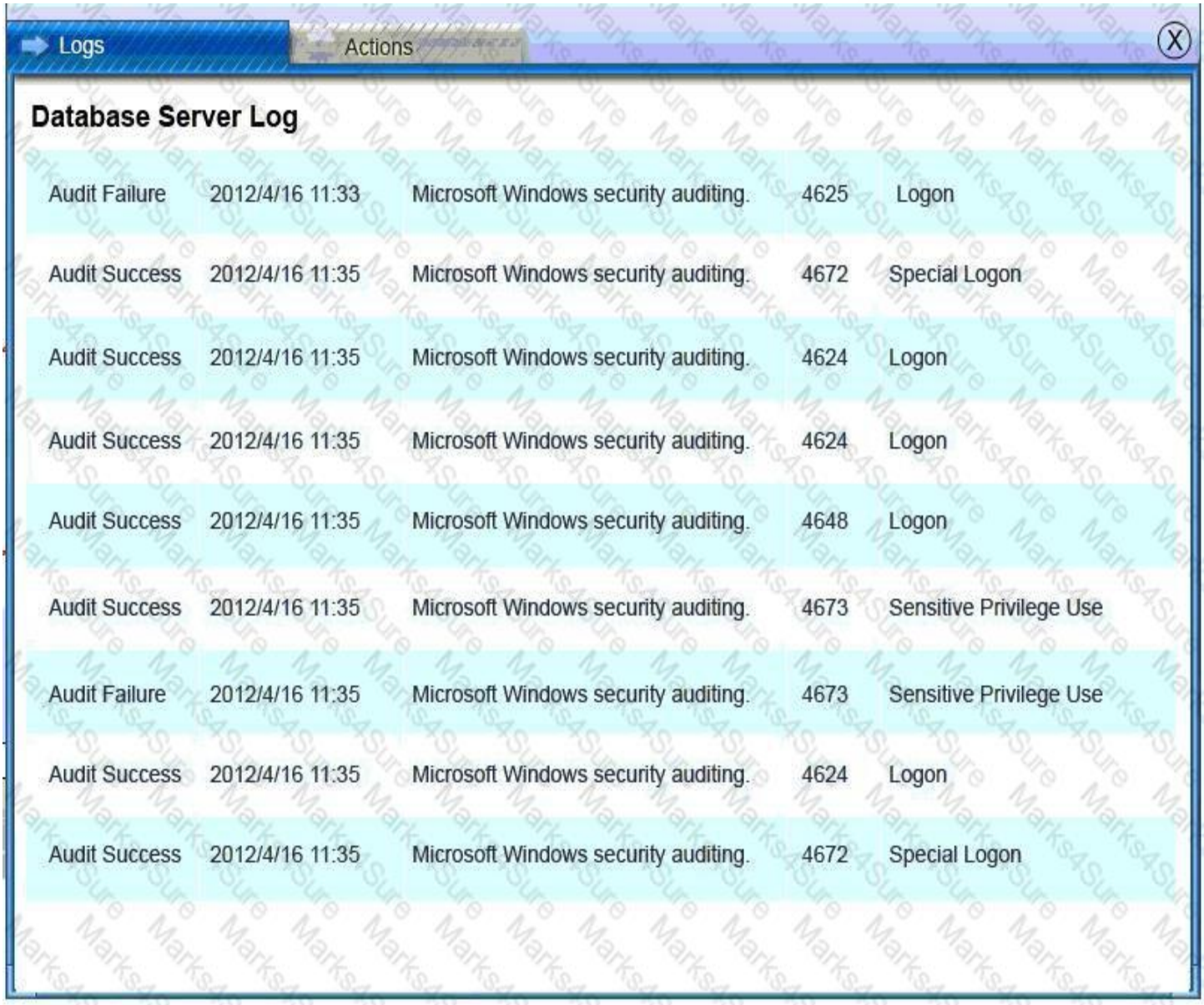


Web Server Log:

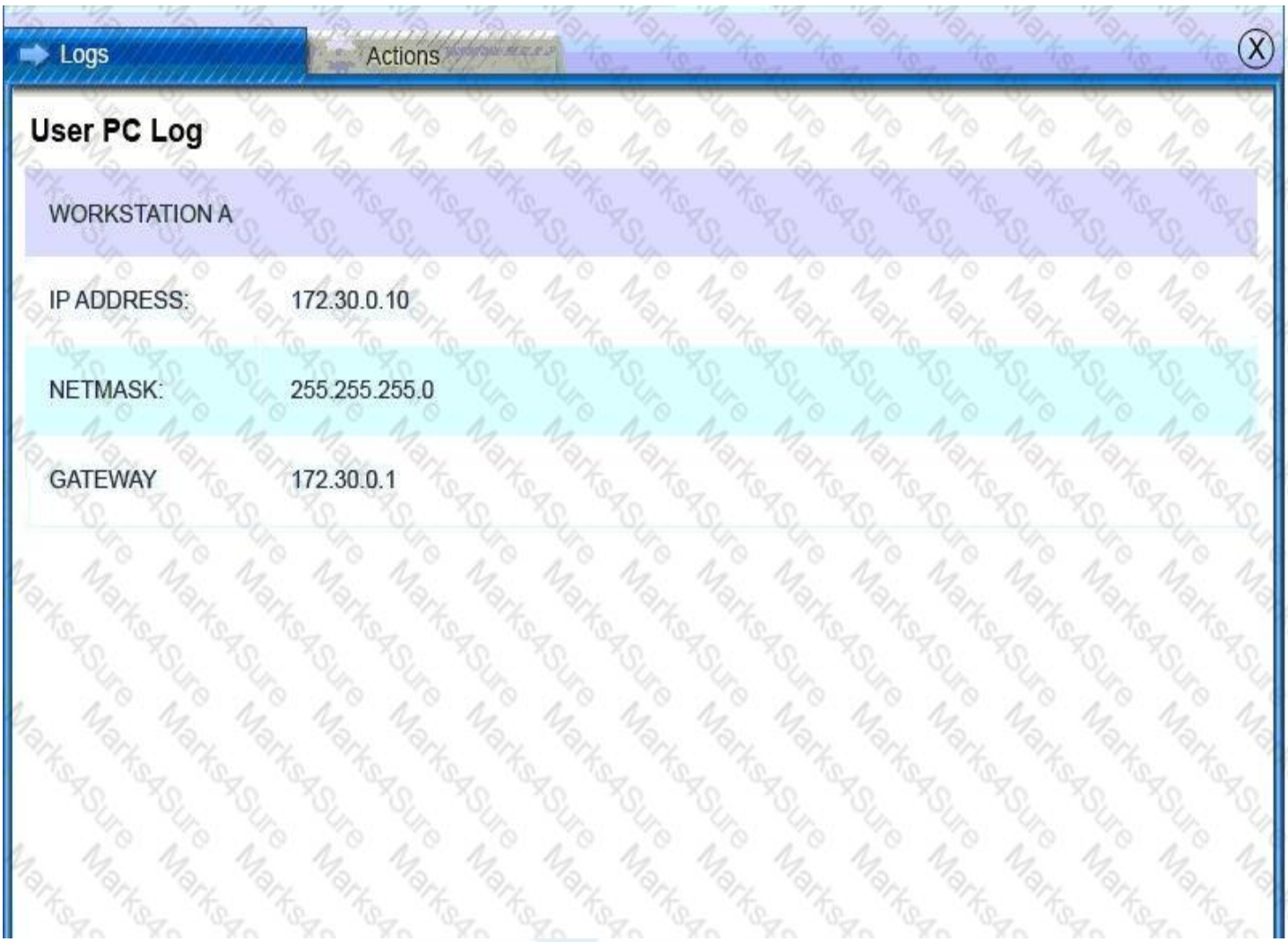

Logs
Actions
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"
123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096 "http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"
123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/



Database Server Log:


Logs
Actions
Database Server Log
Audit Failure 2012/4/16 11:33 Microsoft Windows security auditing. 4625 Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4648 Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Failure 2012/4/16 11:35 Microsoft Windows security auditing. 4673 Sensitive Privilege Use
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4624 Logon
Audit Success 2012/4/16 11:35 Microsoft Windows security auditing. 4672 Special Logon

Users PC Log:



Question #:8 - (Exam Topic 3)

Select the appropriate attack from each drop down list to label the corresponding illustrated attack.

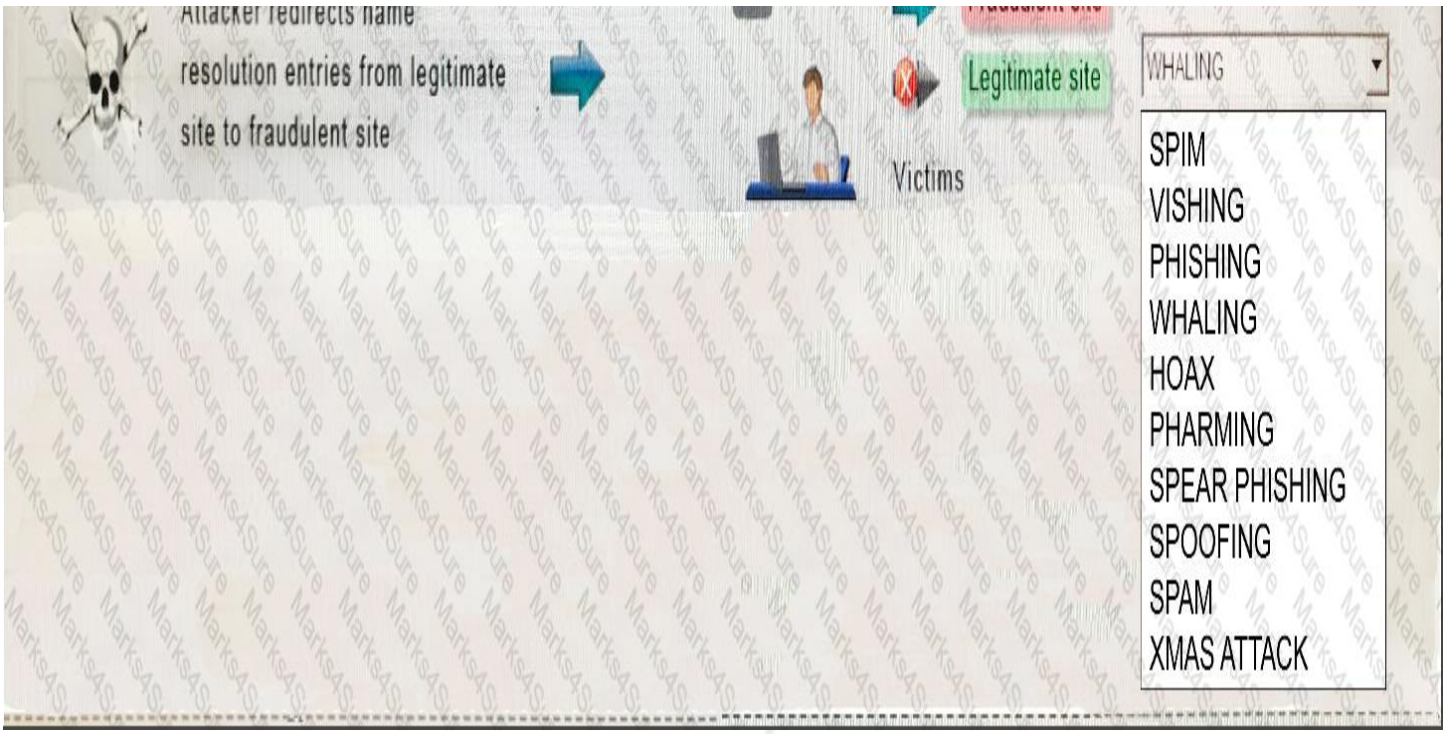
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, SPEAR PHISHING, SPOOFING, SPAM


SPAM
XMAS ATTACK
Attacker collecting credit card details
Phone-based victim
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK
Fraudulent site


Attacker redirects name
resolution entries from legitimate
site to fraudulent site
Legitimate site
Victims
WHALING
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK

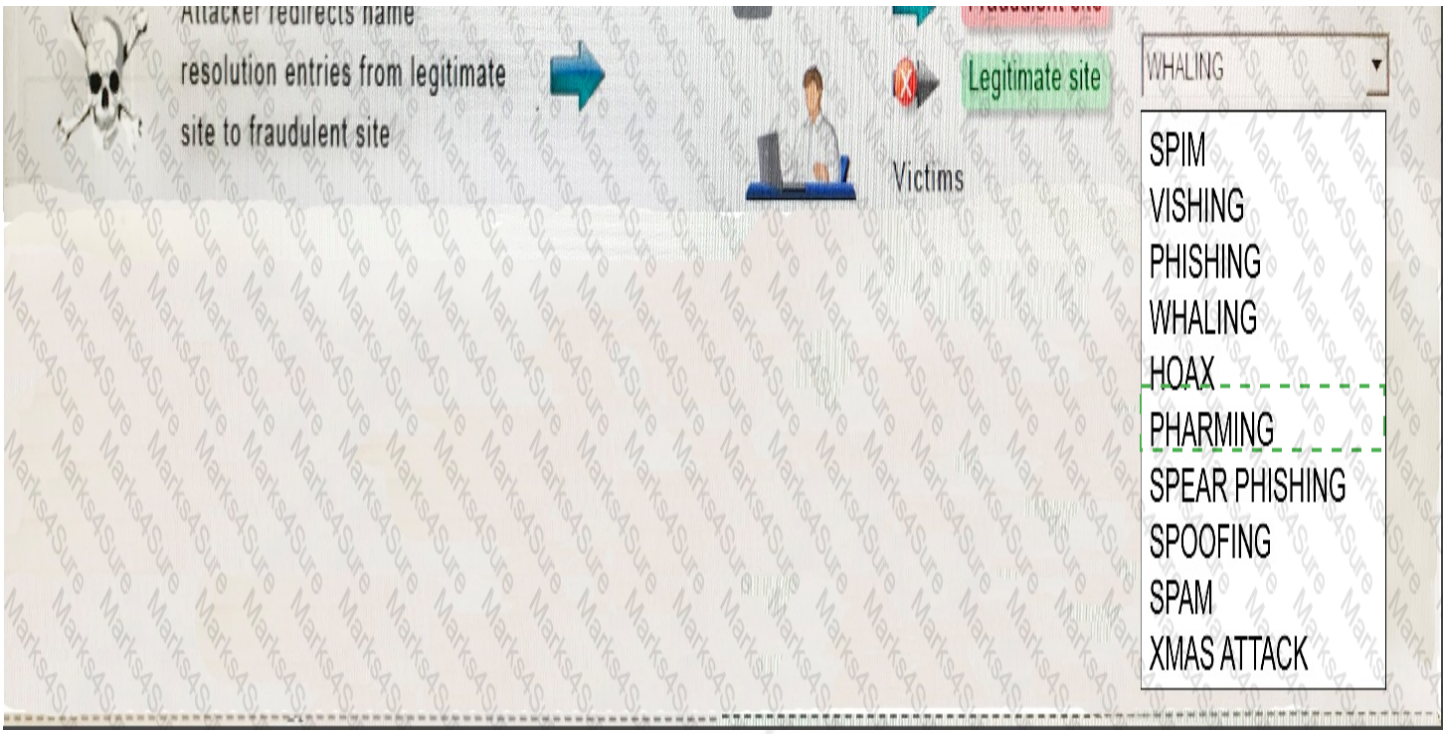
Answer:

Attacks

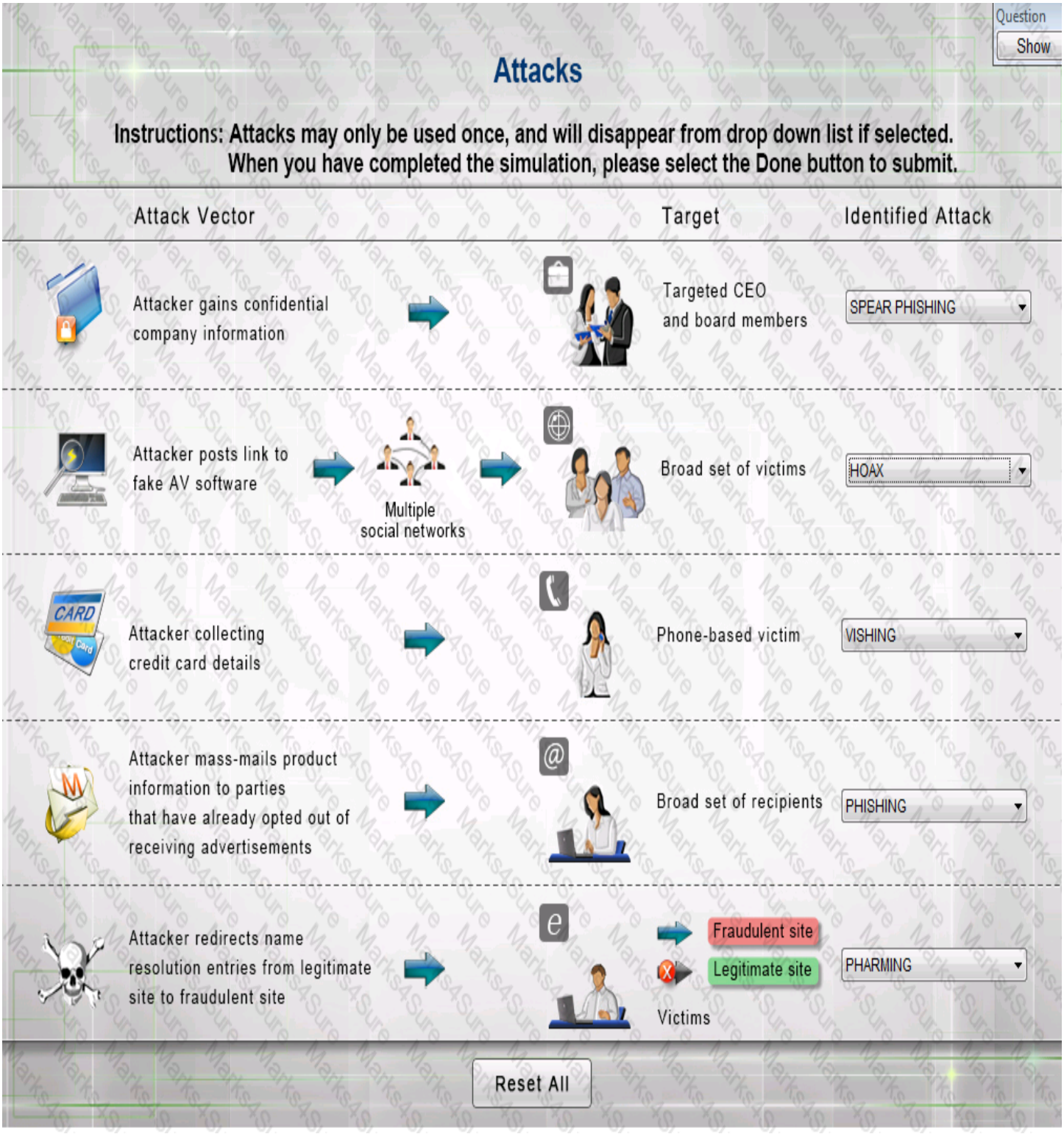
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPIM, VISHING, PHISHING, WHALING, HOAX, PHARMING, **SPEAR PHISHING**, SPOOFING, SPAM, XMAS ATTACK
Attacker posts link to fake AV software (Multiple social networks)	Broad set of victims	SPIM, VISHING, PHISHING, **WHALING**, **HOAX**, PHARMING, SPEAR PHISHING, SPOOFING, SPAM


SPAM
XMAS ATTACK
Attacker collecting credit card details
Phone-based victim
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK
Fraudulent site



Explanation



1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:

http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

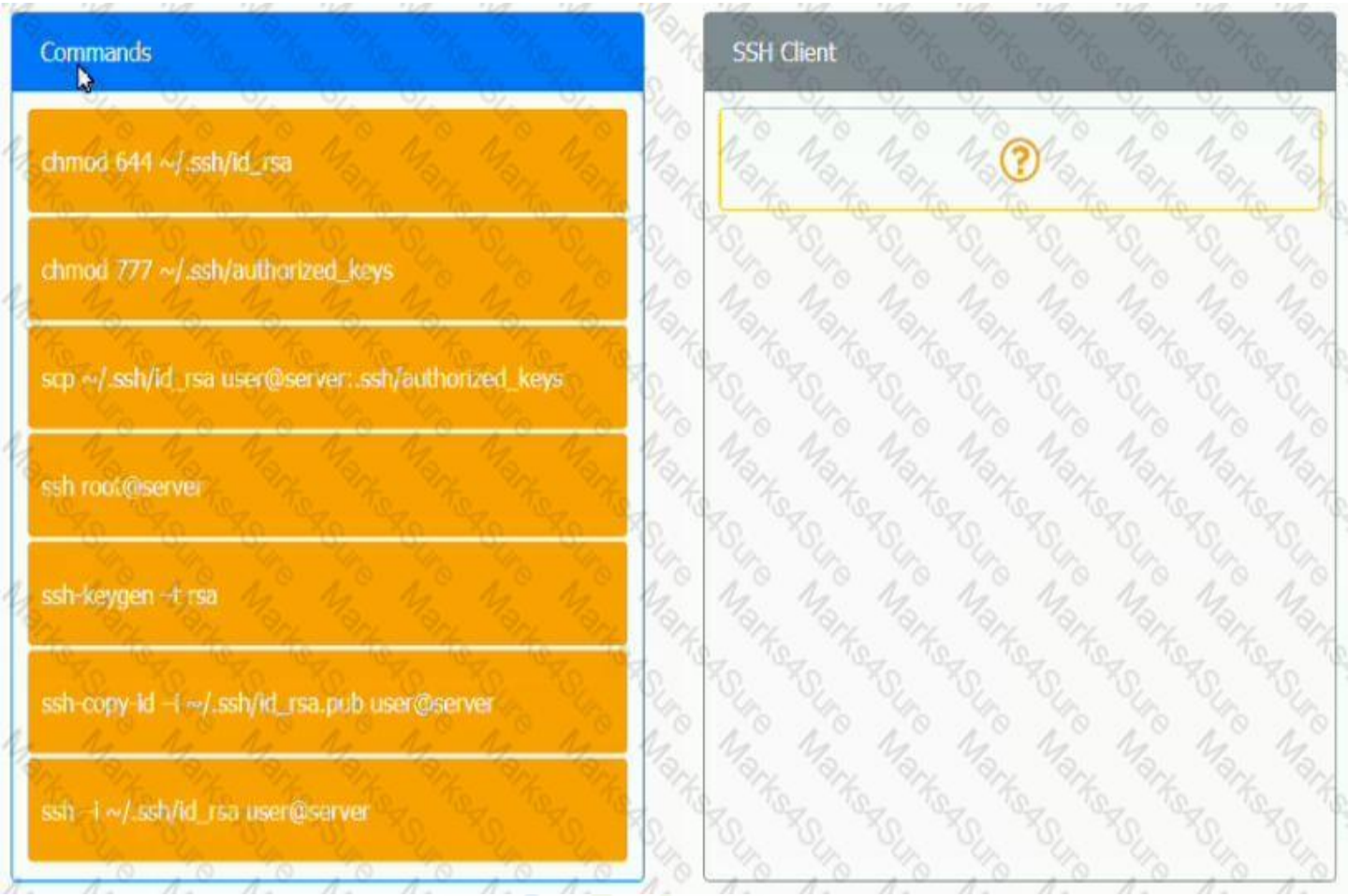
Question #:9 - (Exam Topic 3)

A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

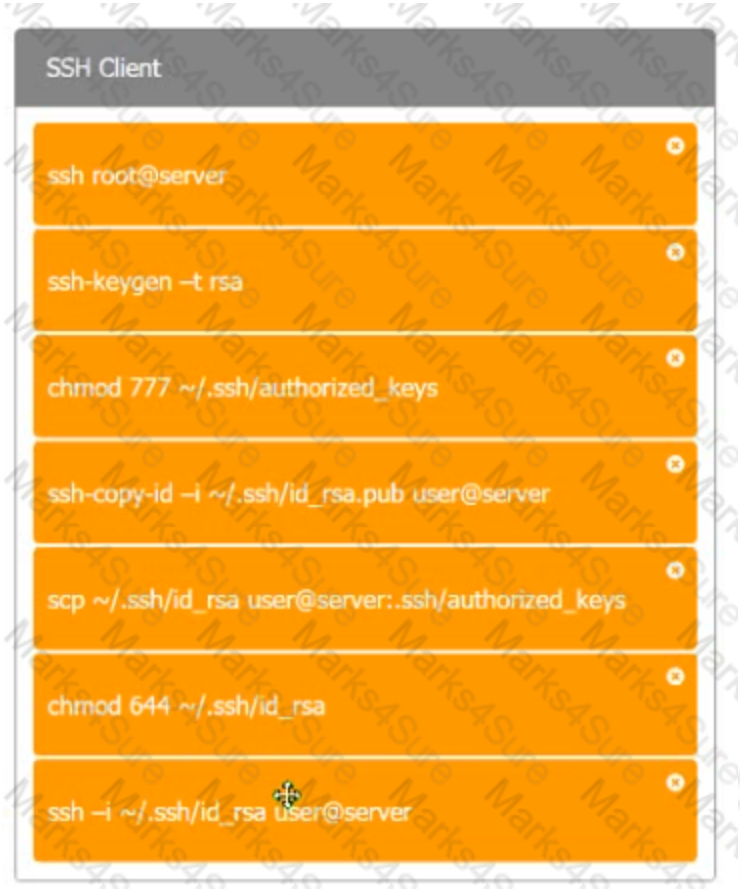
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Commands
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen -t rsa
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
ssh -i ~/.ssh/id_rsa user@server
SSH Client

Answer:

Explanation



Question #:10 - (Exam Topic 3)

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS:

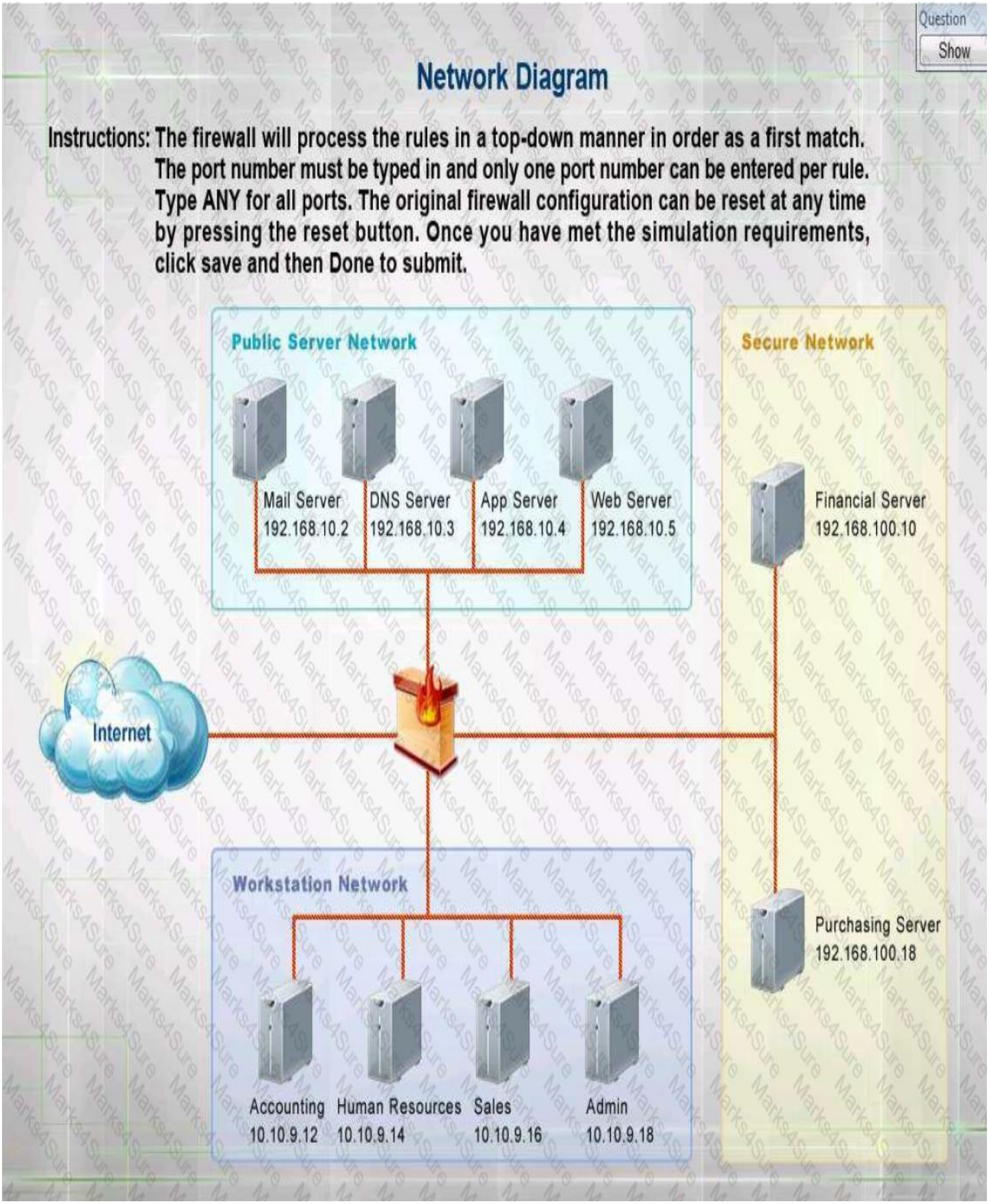
Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.

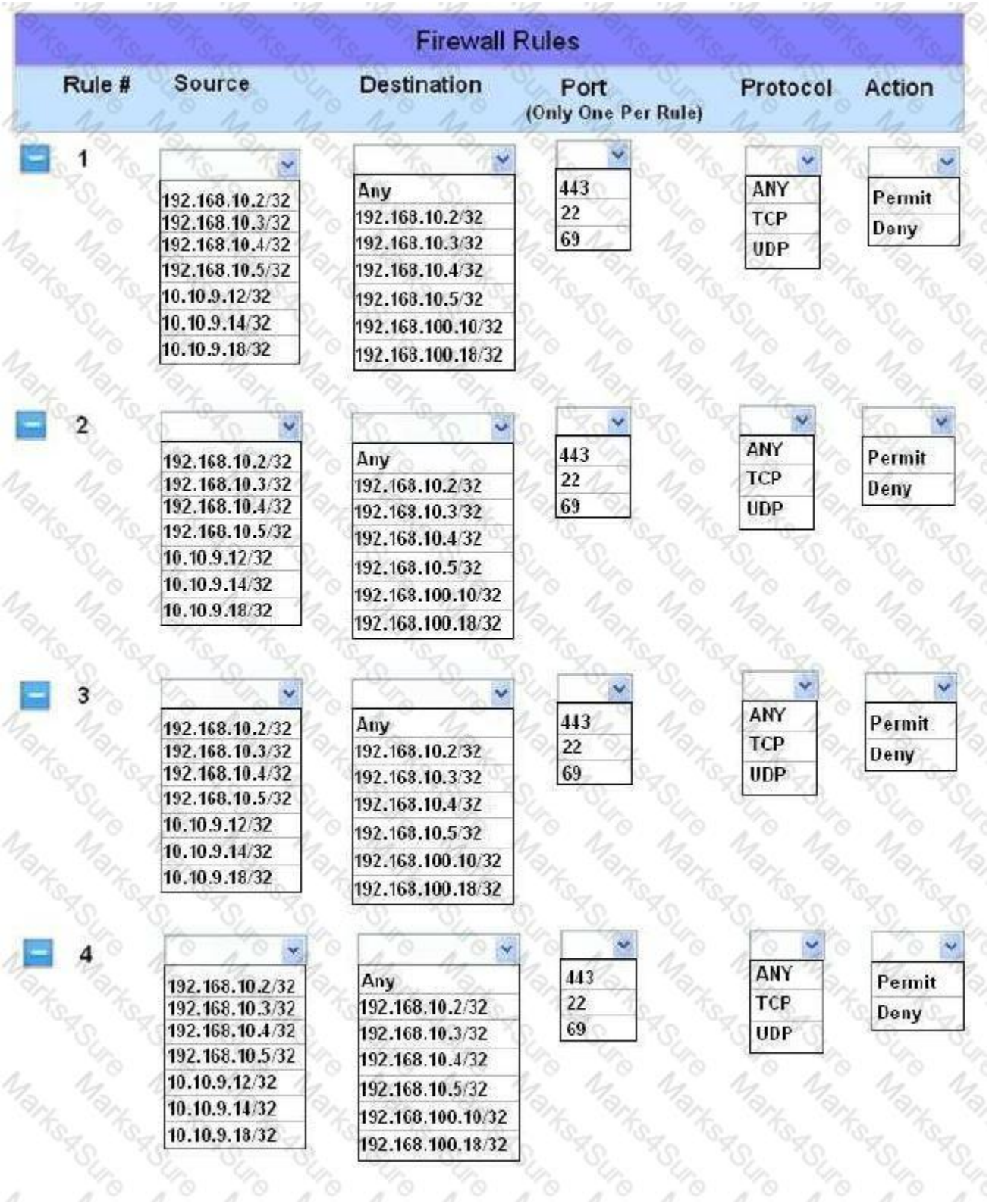
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port

3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

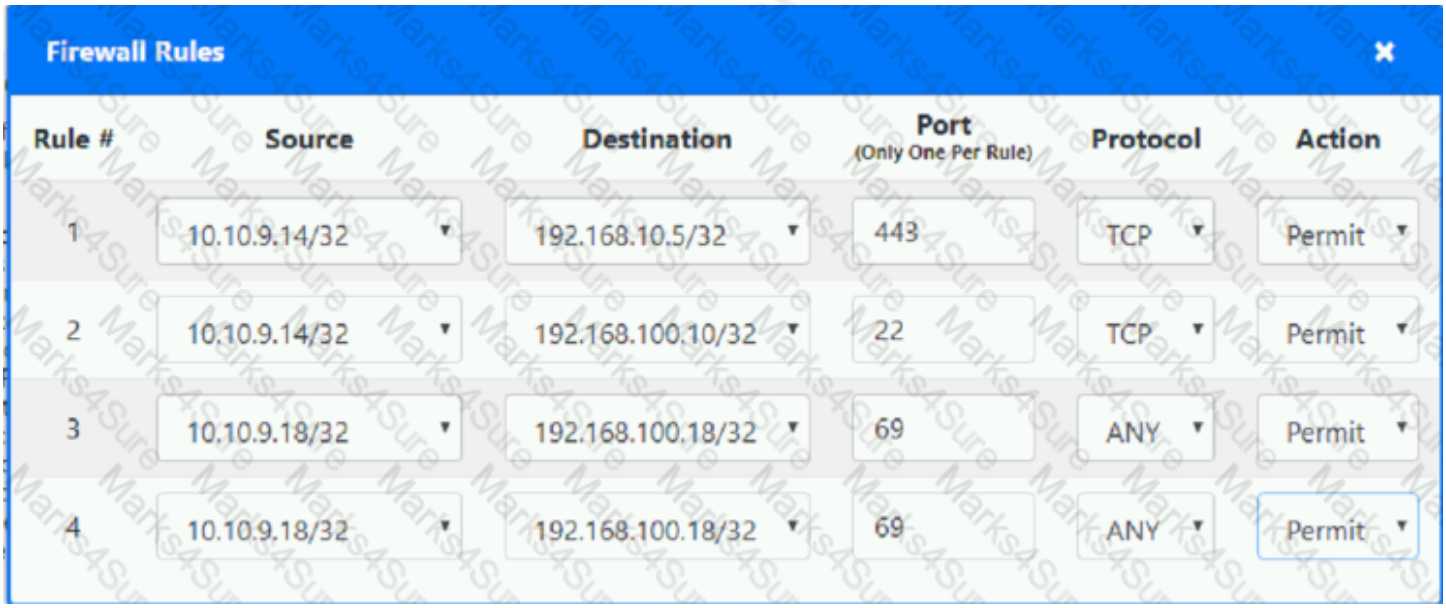

Question
Show
Network Diagram
Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.
Public Server Network
Mail Server 192.168.10.2
DNS Server 192.168.10.3
App Server 192.168.10.4
Web Server 192.168.10.5
Secure Network
Financial Server 192.168.100.10
Internet
Workstation Network
Purchasing Server 192.168.100.18
Accounting 10.10.9.12
Human Resources 10.10.9.14
Sales 10.10.9.16
Admin 10.10.9.18

Hot Area:



Answer:

Explanation



Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References:Stewart,

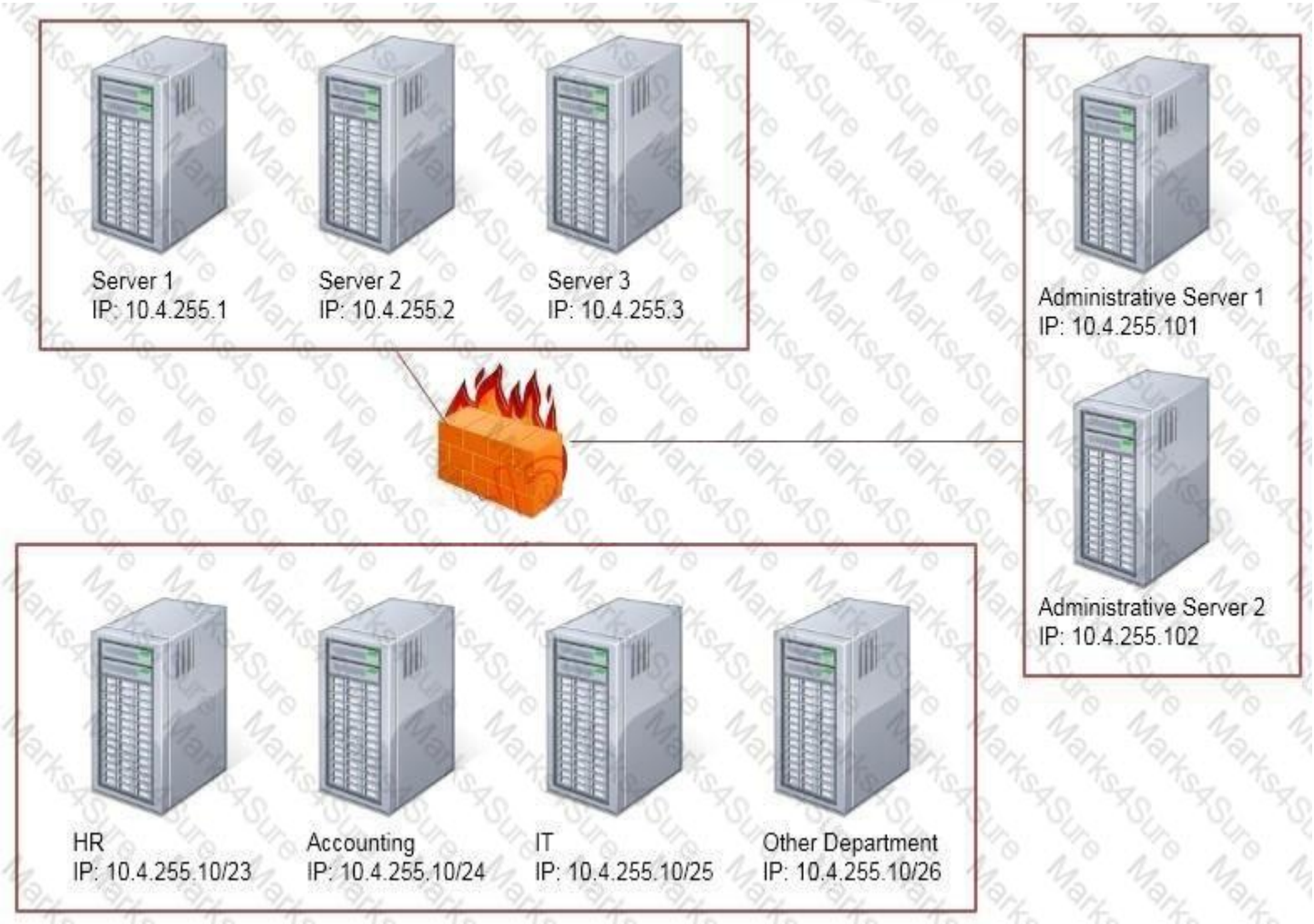
James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question #:11 - (Exam Topic 3)

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

See the solution below.

Explanation

Use the following answer for this simulation task.

Below table has all the answers required for this question.

Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny
10.4.255.10/24	10.4.255.101	443	TCP	Allow
10.4.255.10/23	10.4.255.2	22	TCP	Allow
10.4.255.10/25	10.4.255.101	Any	Any	Allow
10.4.255.10/25	10.4.255.102	Any	Any	Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.

Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.

When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.

The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.

The primary purpose of UDP is to send small packets of information.

The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections? HTTPS and is a TCP port.

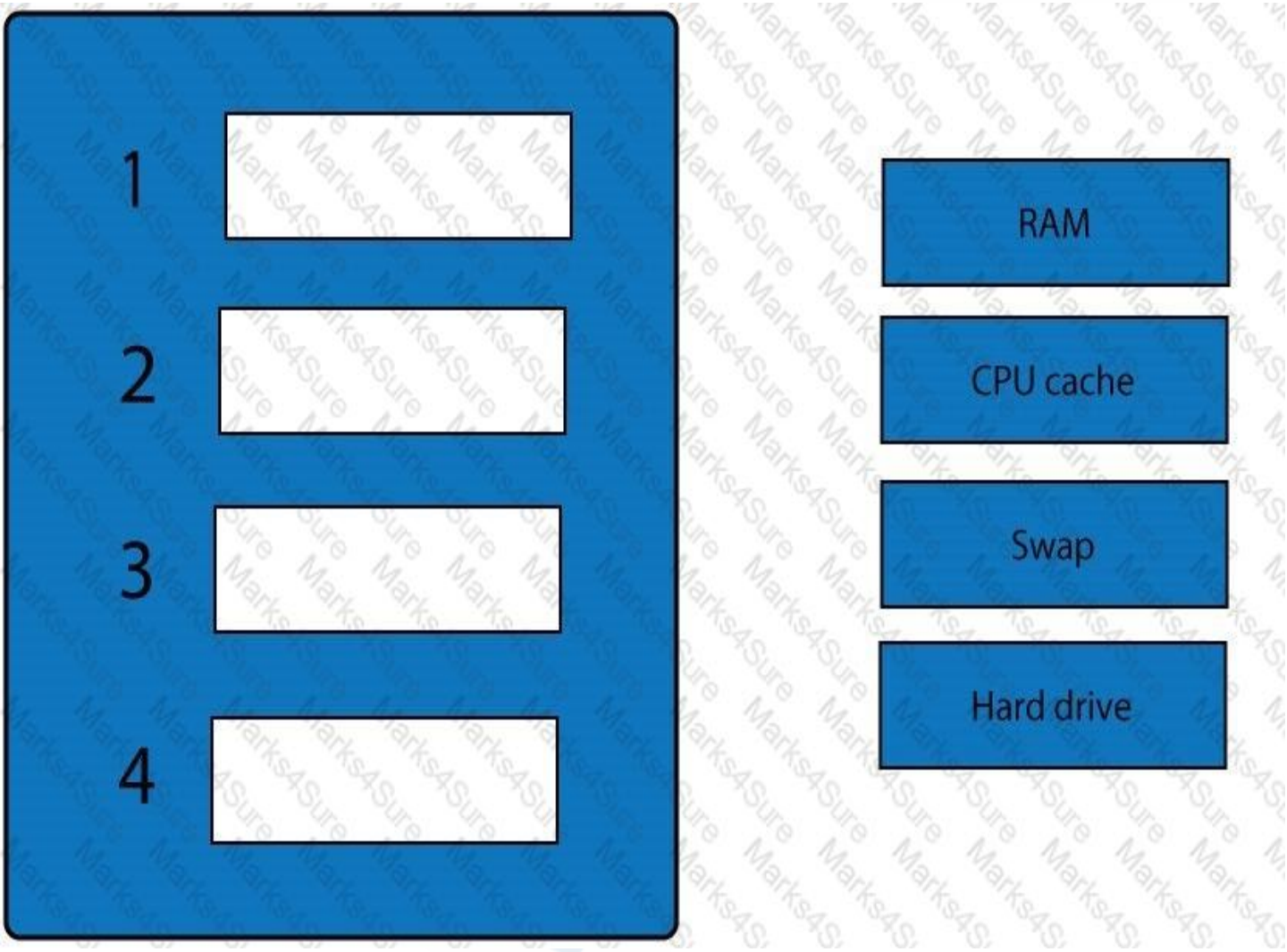
Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

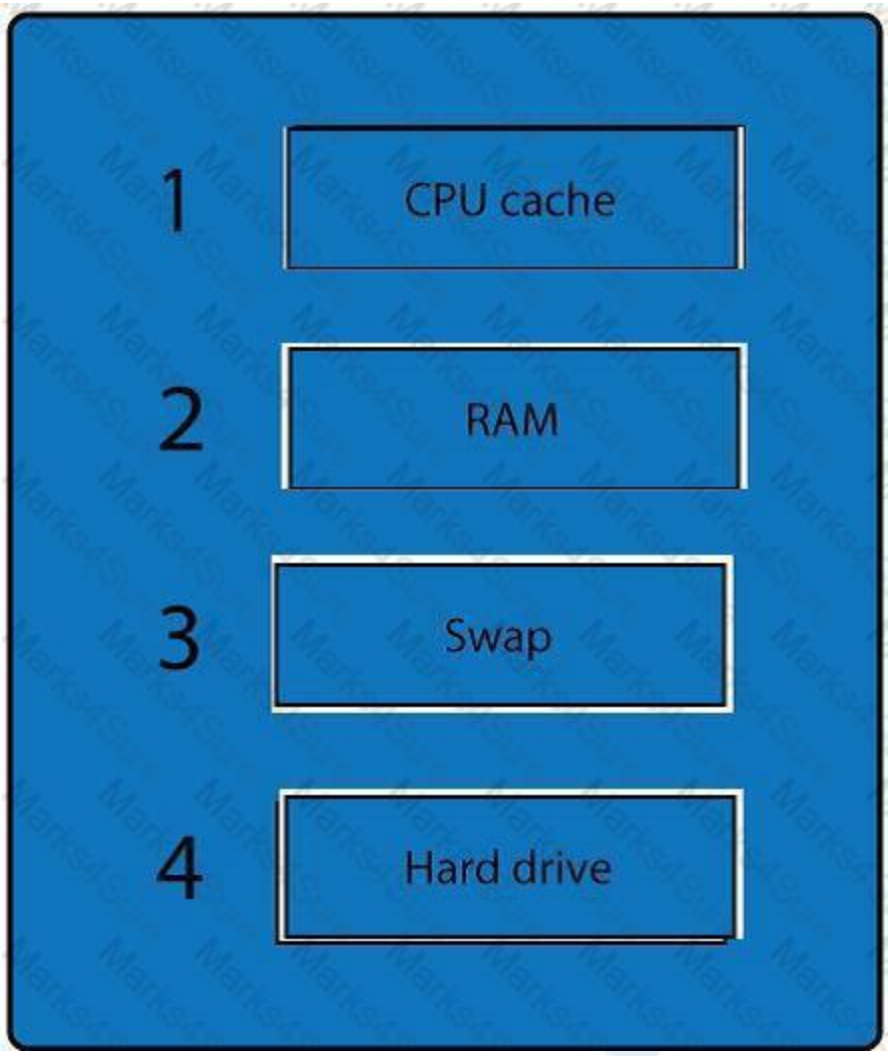
Question #:12 - (Exam Topic 3)

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.



Answer:

Explanation



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

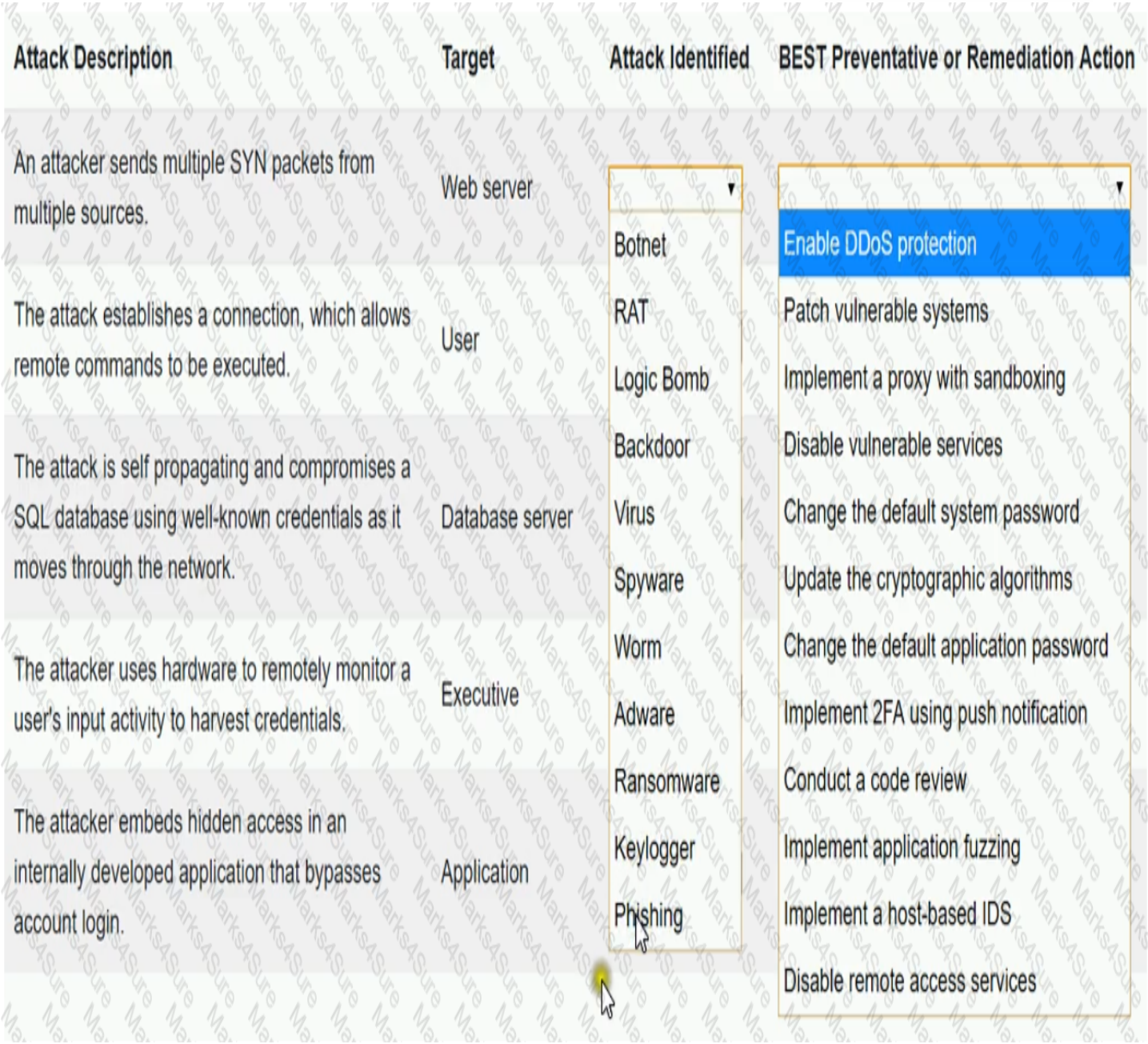
Question #:13 - (Exam Topic 3)

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

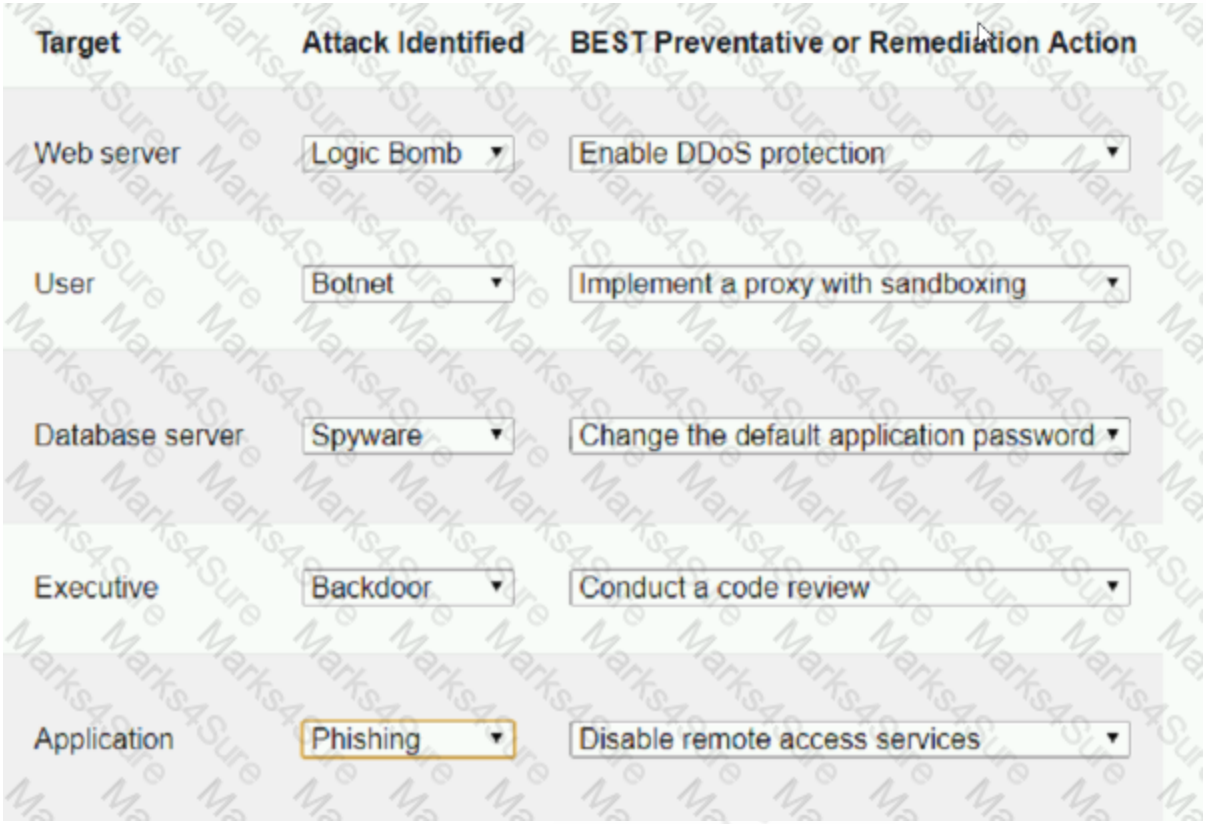
Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server		
The attack establishes a connection, which allows remote commands to be executed.	User		
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server		
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive		
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application		



check the answer below.

Explanation

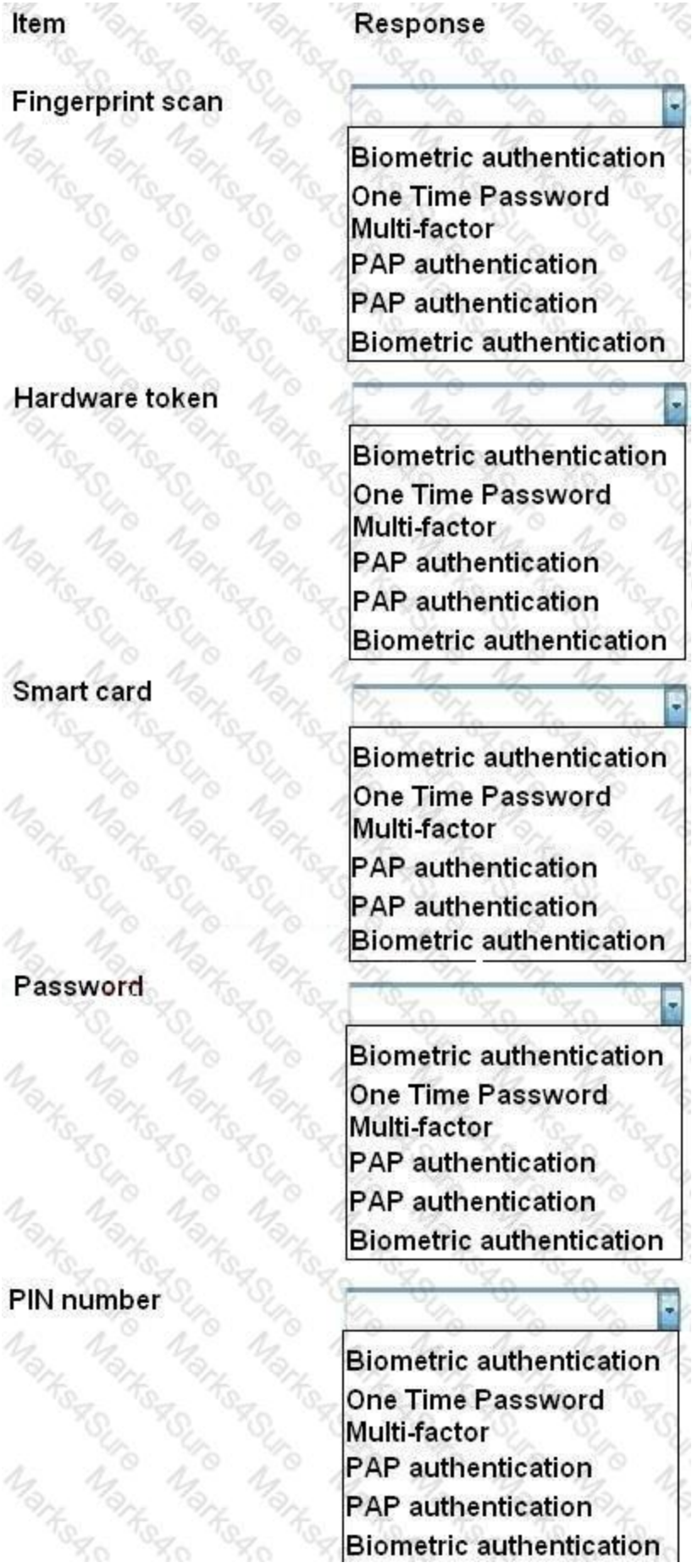
Use the following settings for answer this simulation question.

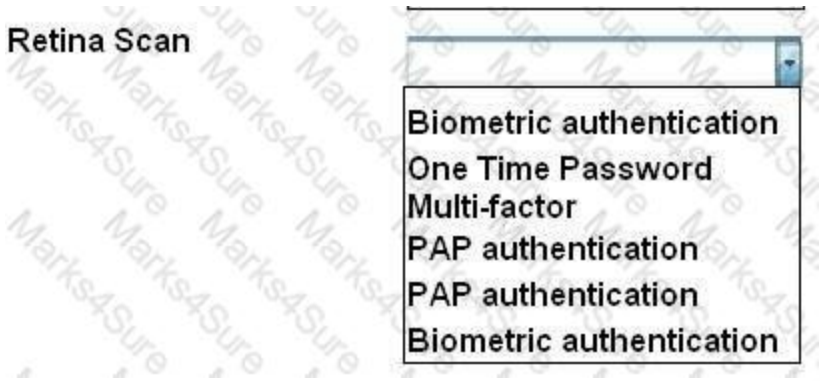


Question #:14 - (Exam Topic 3)

For each of the given items, select the appropriate authentication category from the drop down choices.

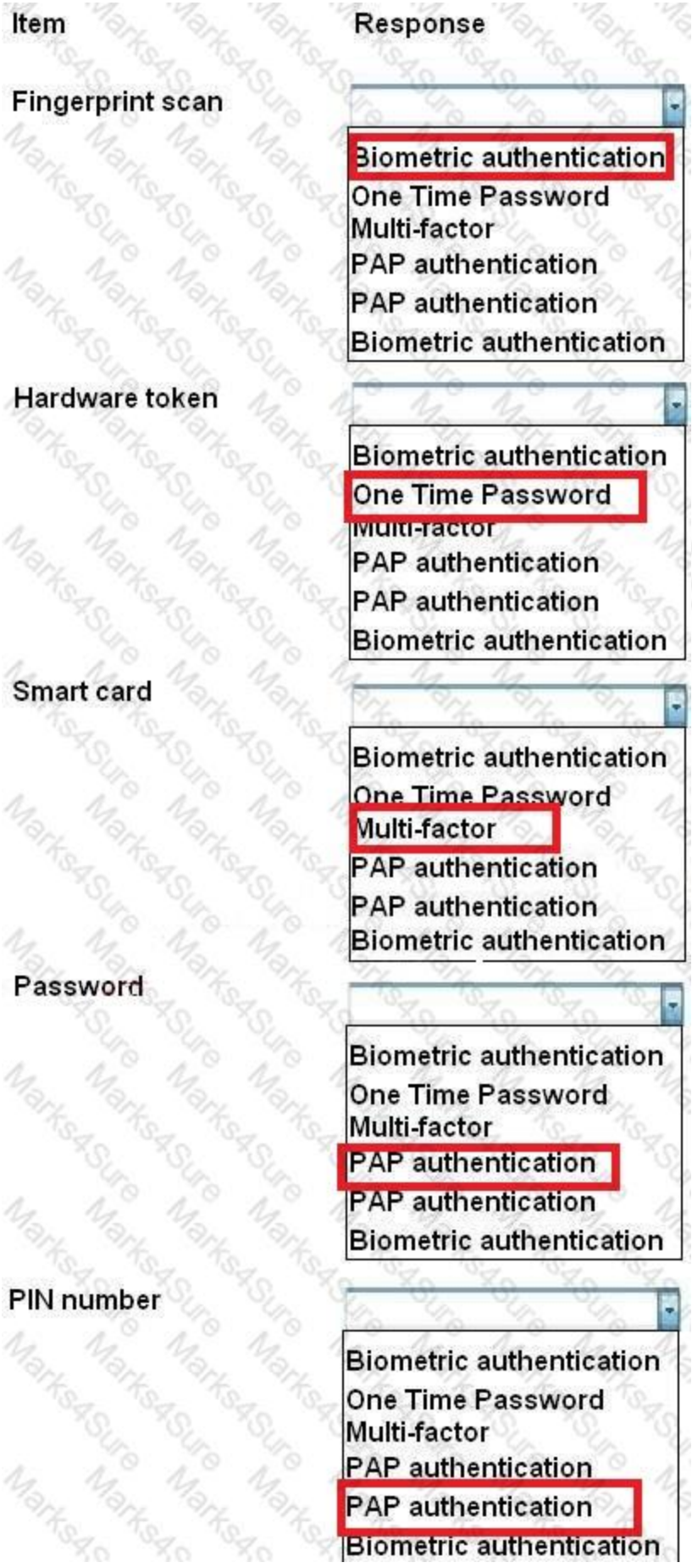
Select the appropriate authentication type for the following items:

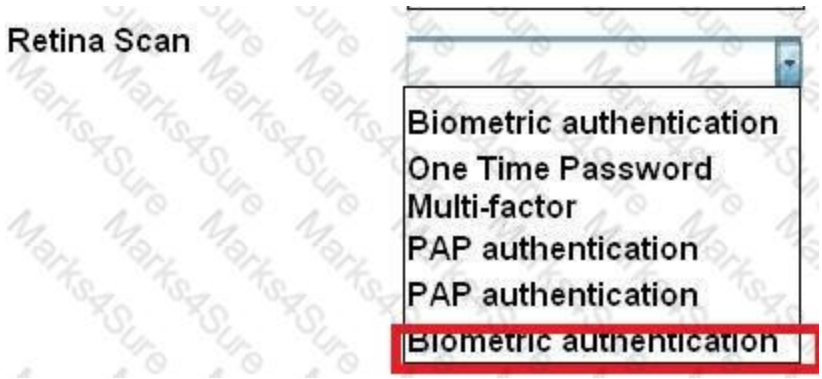

Item
Response
Fingerprint scan
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
Hardware token
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
Smart card
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
Password
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
PIN number
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication



Answer:

Explanation


Item
Response
Fingerprint scan
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
Hardware token
Biometric authentication
One Time Password
PAP authentication
PAP authentication
Biometric authentication
Smart card
Biometric authentication
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
Password
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication
PIN number
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication



Question #:15 - (Exam Topic 3)

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	Something you have / Something you know / Something you are / All given authentication categories
Smart card	Something you have / Something you know / Something you are / All given authentication categories
Hardware Token	Something you have / Something you know / Something you are / All given authentication categories
Password	Something you have / Something you know / Something you are / All given authentication categories
PIN number	Something you have / Something you know / Something you are / All given authentication categories
Fingerprint scan	Something you have / Something you know / Something you are / All given authentication categories

Something you are

All given authentication categories

Answer:

Explanation

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	Something you have / Something you know / **Something you are** / All given authentication categories
Smart card	**Something you have** / Something you know / Something you are / All given authentication categories
Hardware Token	**Something you have** / Something you know / Something you are / All given authentication categories
Password	Something you have / **Something you know** / Something you are / All given authentication categories
PIN number	Something you have / **Something you know** / Something you are / All given authentication categories
Fingerprint scan	Something you have / Something you know / Something you are

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

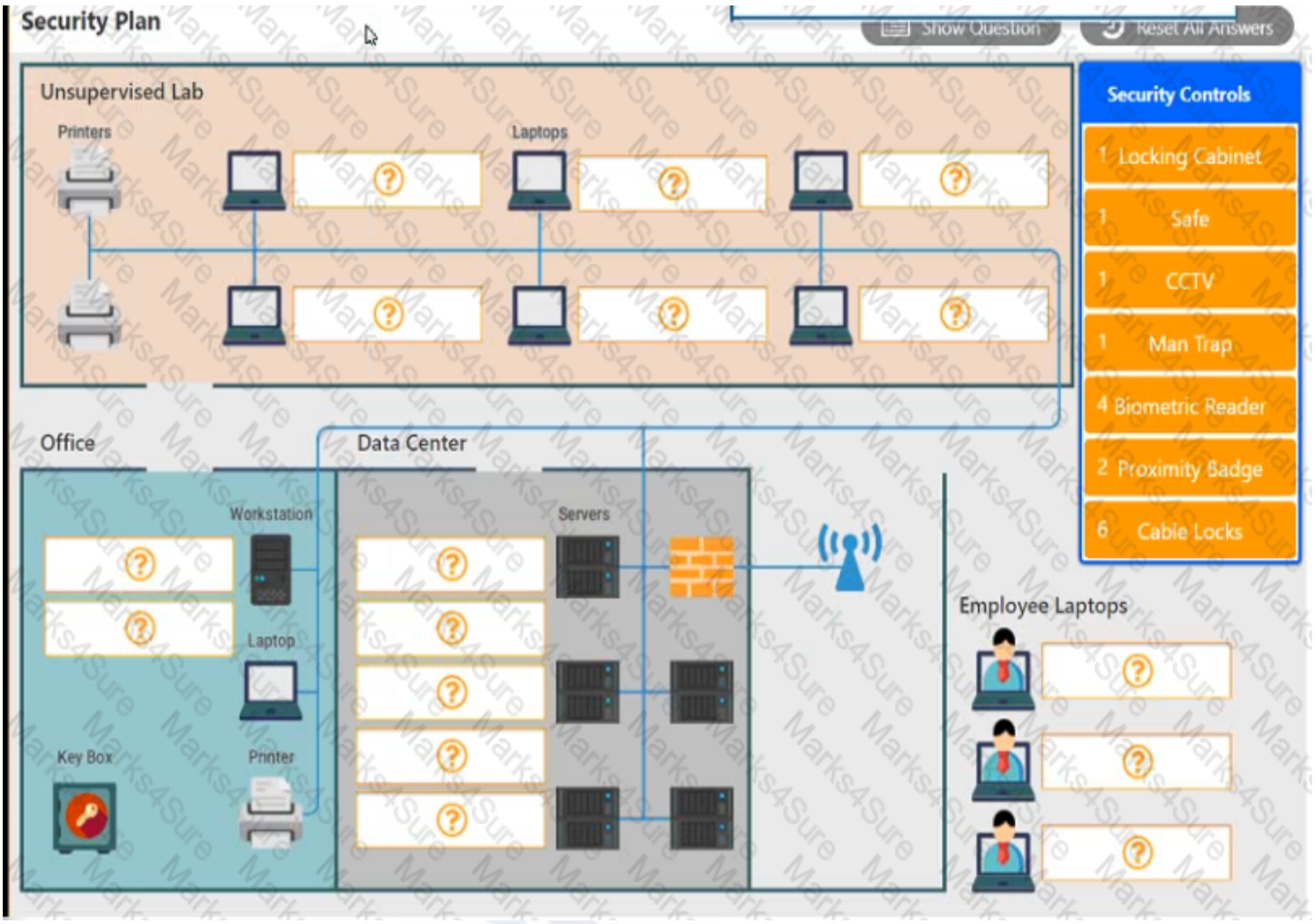
Something

you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

Question #:16 - (Exam Topic 3)

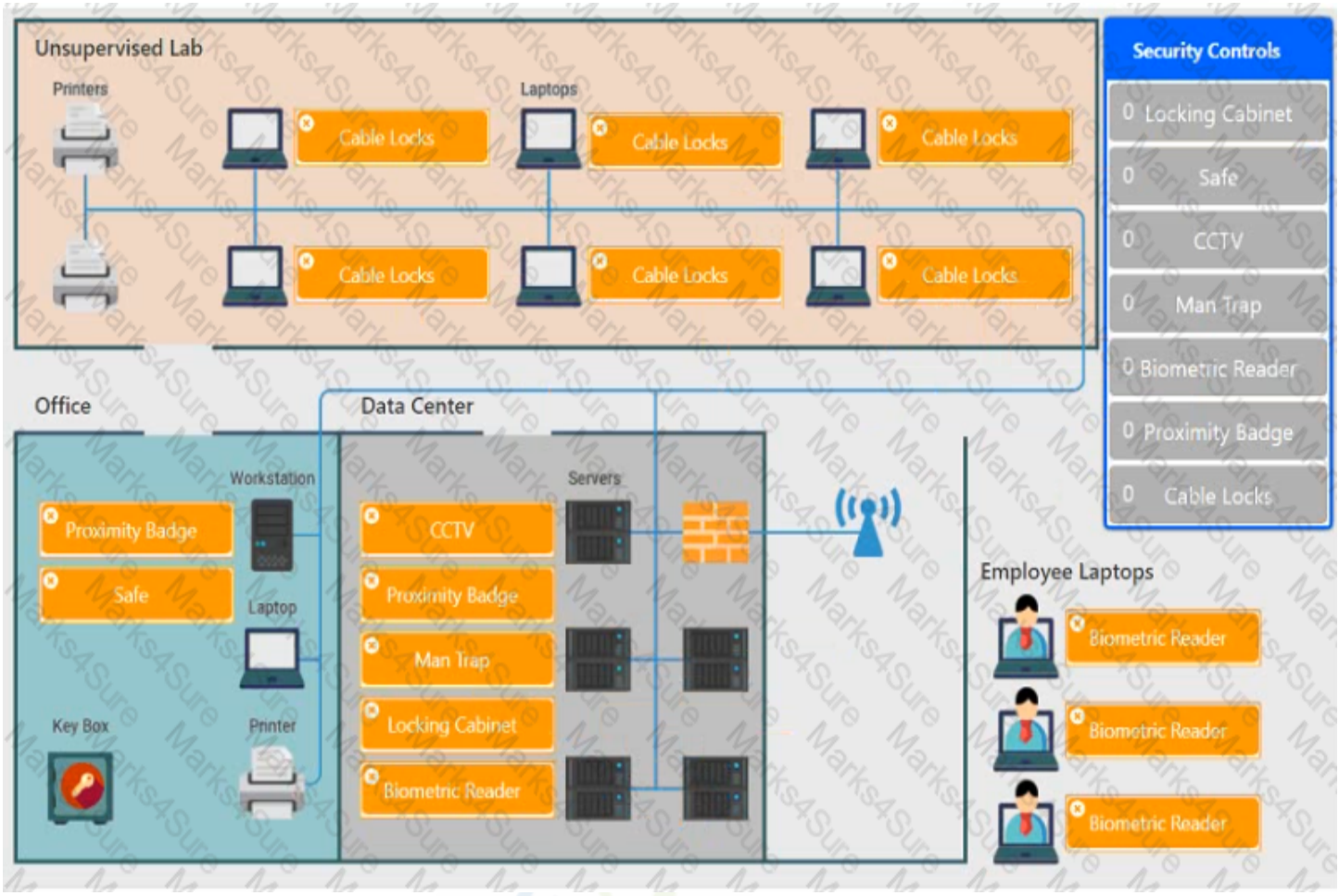
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.



Answer:

Explanation



Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader

Safe is a hardware/physical security measure

Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.

Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artifacts.

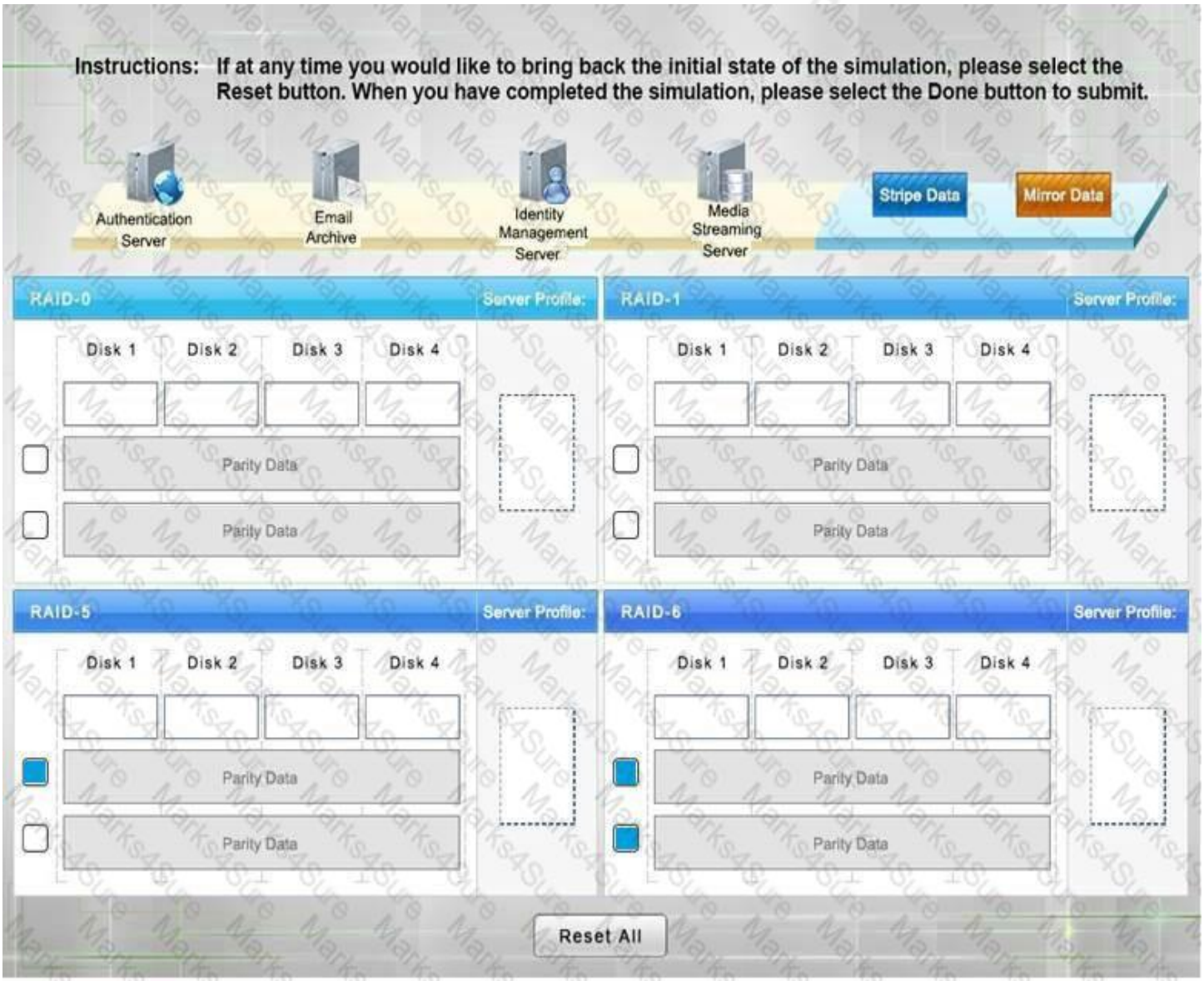
Question #:17 - (Exam Topic 3)

A security administrator is given the security and availability profiles for servers that are being deployed.

- Match each RAID type with the correct configuration and MINIMUM number of drives.
- Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:
- All drive definitions can be dragged as many times as necessary

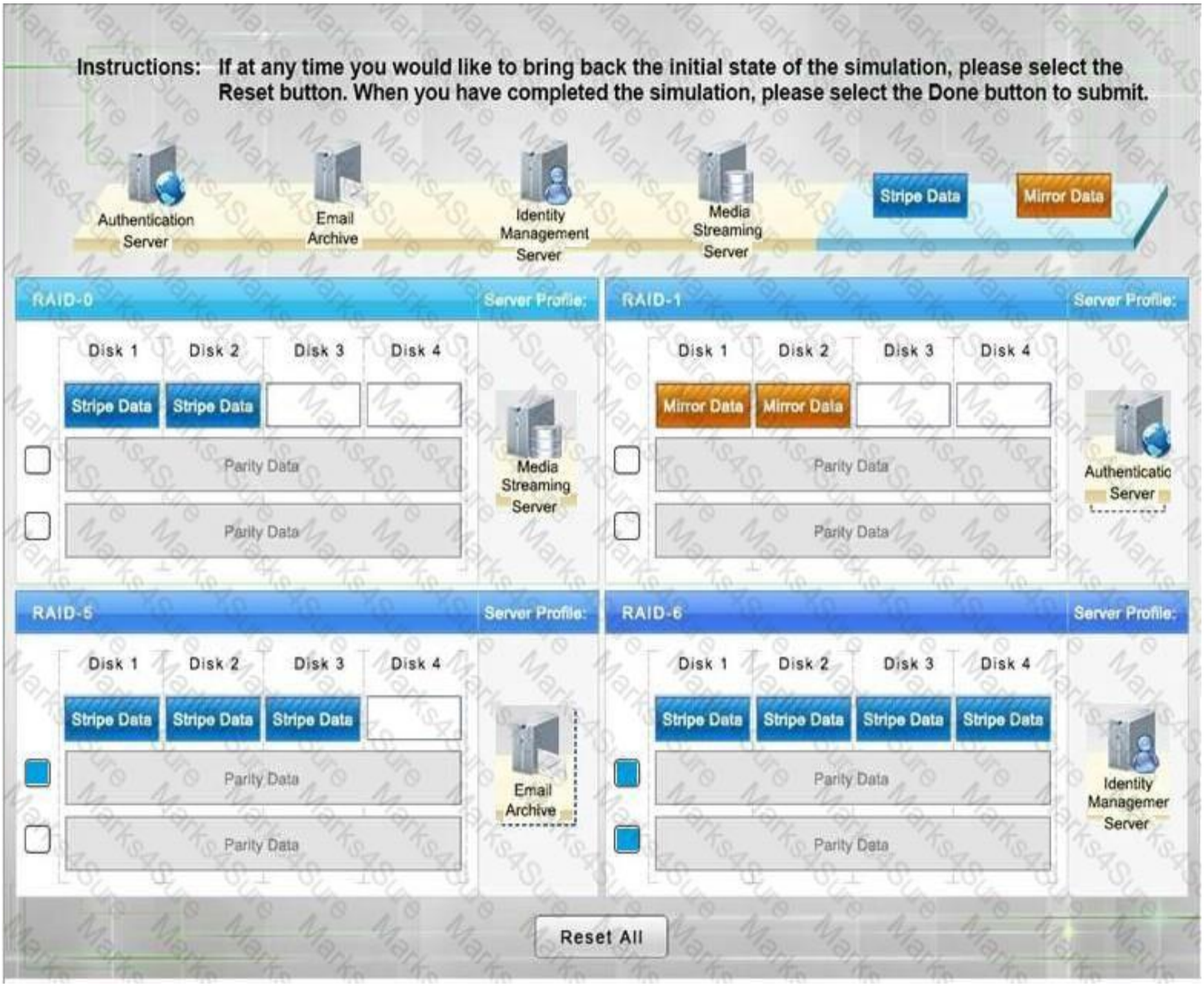
- Not all placeholders may be filled in the RAID configuration boxes
- If parity is required, please select the appropriate number of parity checkboxes
- Server profiles may be dragged only once

If at any time you would like to bring back the initial state of the simulation, please select the Reset 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.



Answer:

Explanation



RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity.

RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.

RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.

RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

http://www.adaptec.com/en-us/solutions/raid_levels.html

Question #:18 - (Exam Topic 3)

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

Answer:

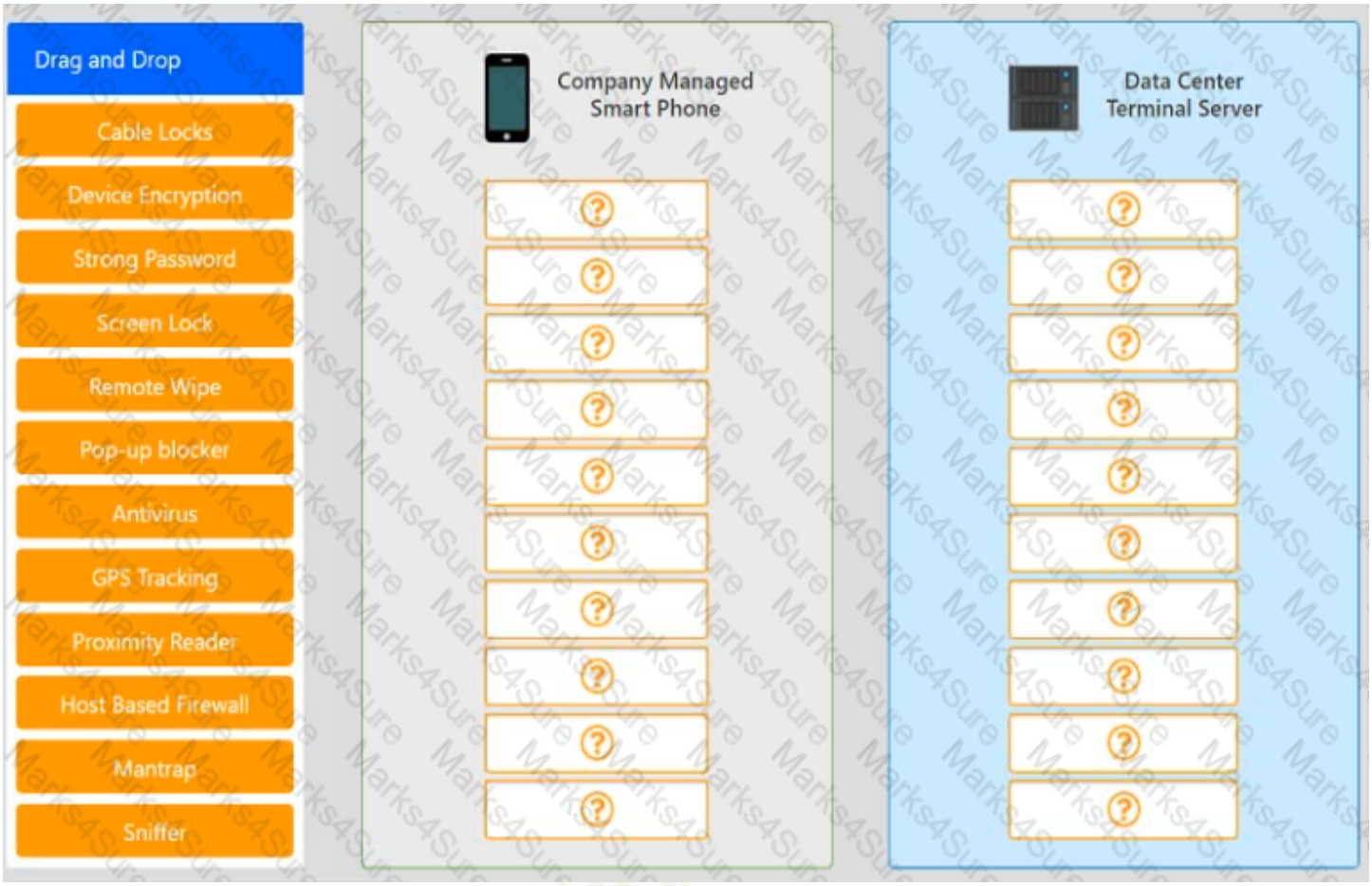
Explanation

Question #:19 - (Exam Topic 3)

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.

Drag and drop the applicable controls to each asset types?

Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

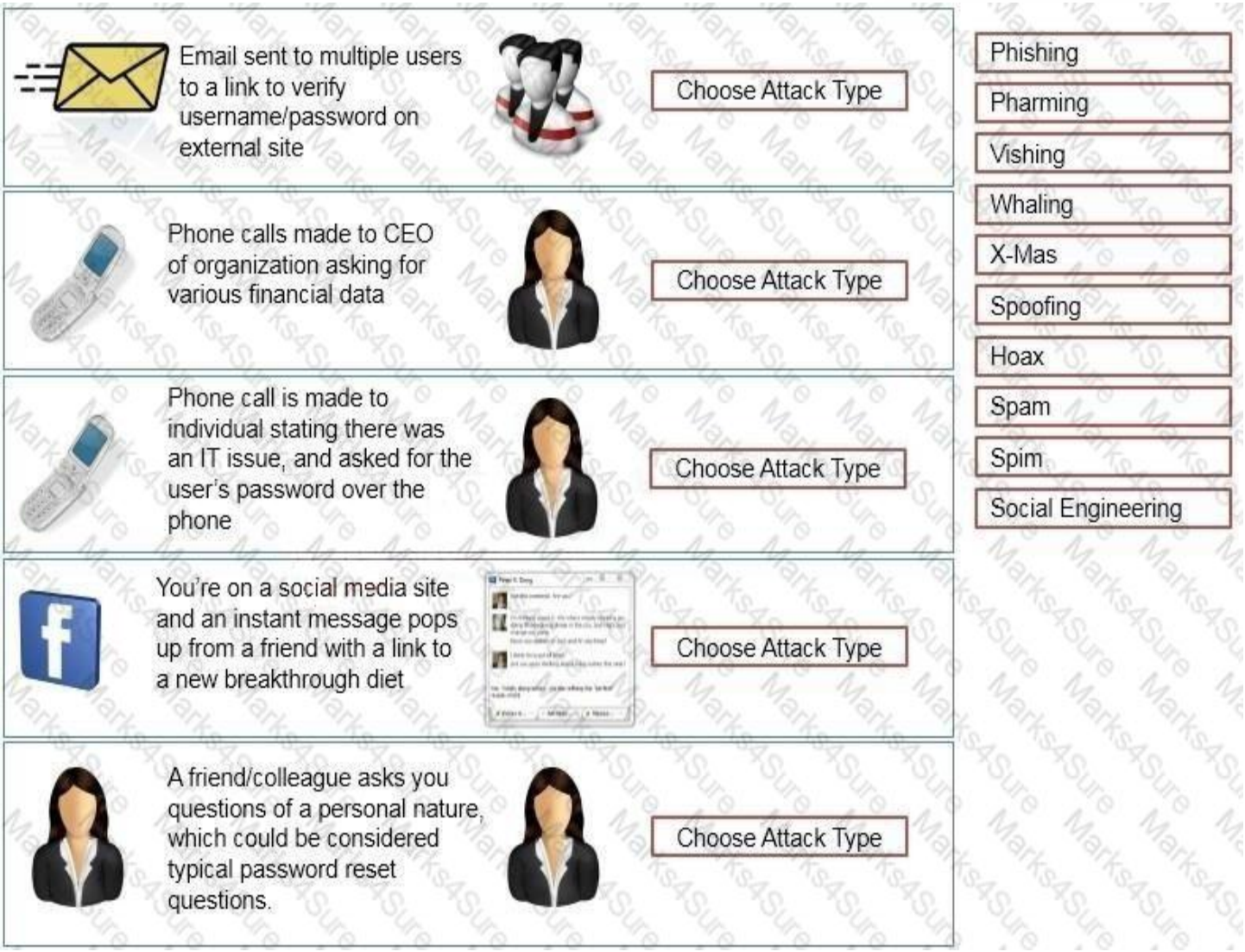


Answer:

Explanation

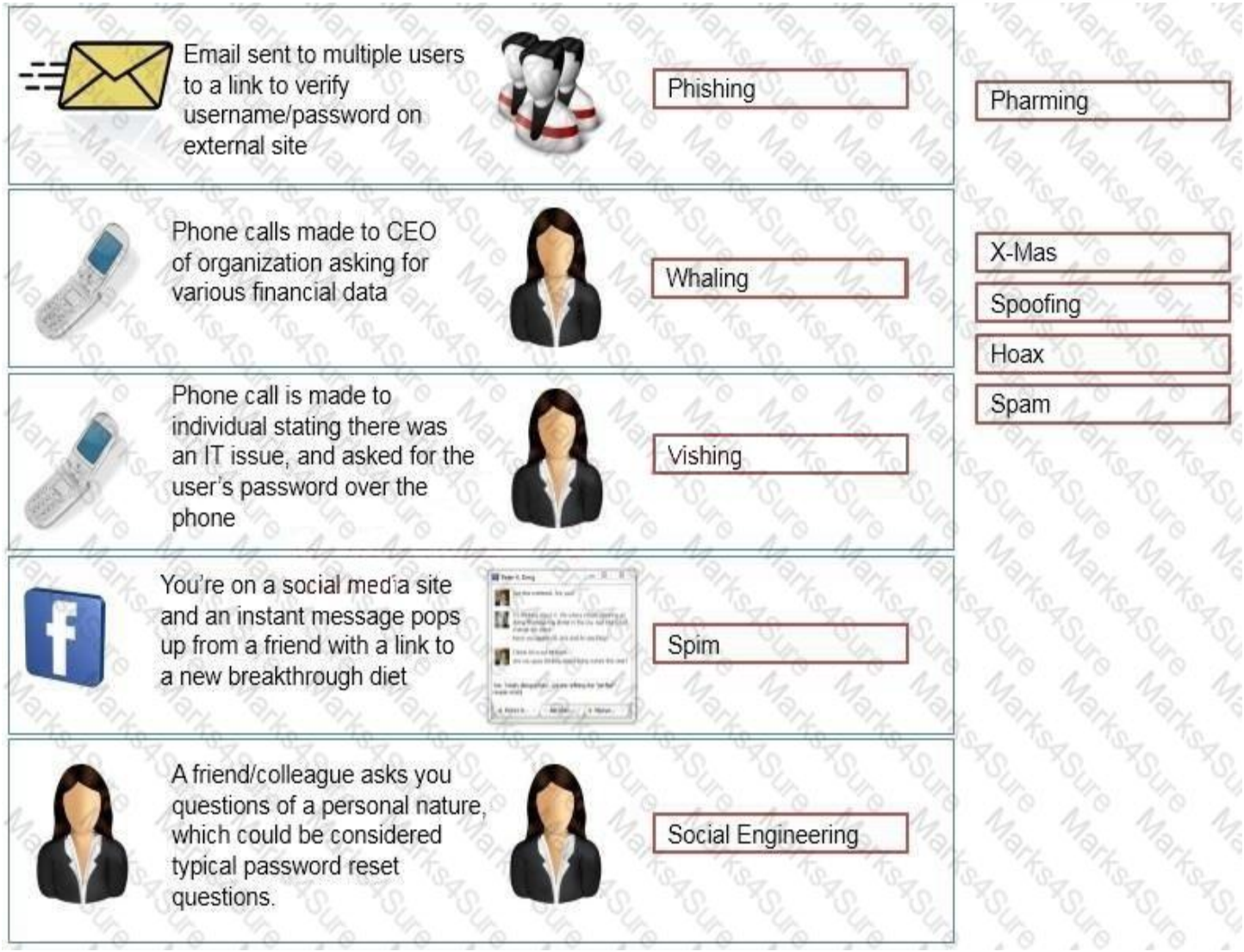
Question #:20 - (Exam Topic 3)

Task: Determine the types of attacks below by selecting an option from the dropdown list.



Answer:

Explanation



A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private

information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS)

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

http://www.webopedia.com/TERM/P/phishing.html

http://www.techopedia.com/definition/28643/whaling

http://www.webopedia.com/TERM/V/vishing.html

http://searchsecurity.techtarget.com/definition/social-engineering

Question #:21 - (Exam Topic 3)

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

• Hostname: ws01

• Domain: comptia.org

• IPv4: 10.1.9.50

• IPV4: 10.2.10.50

• Root: home.aspx

• DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.

Answer:

Explanation

Question #:22 - (Exam Topic 3)

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

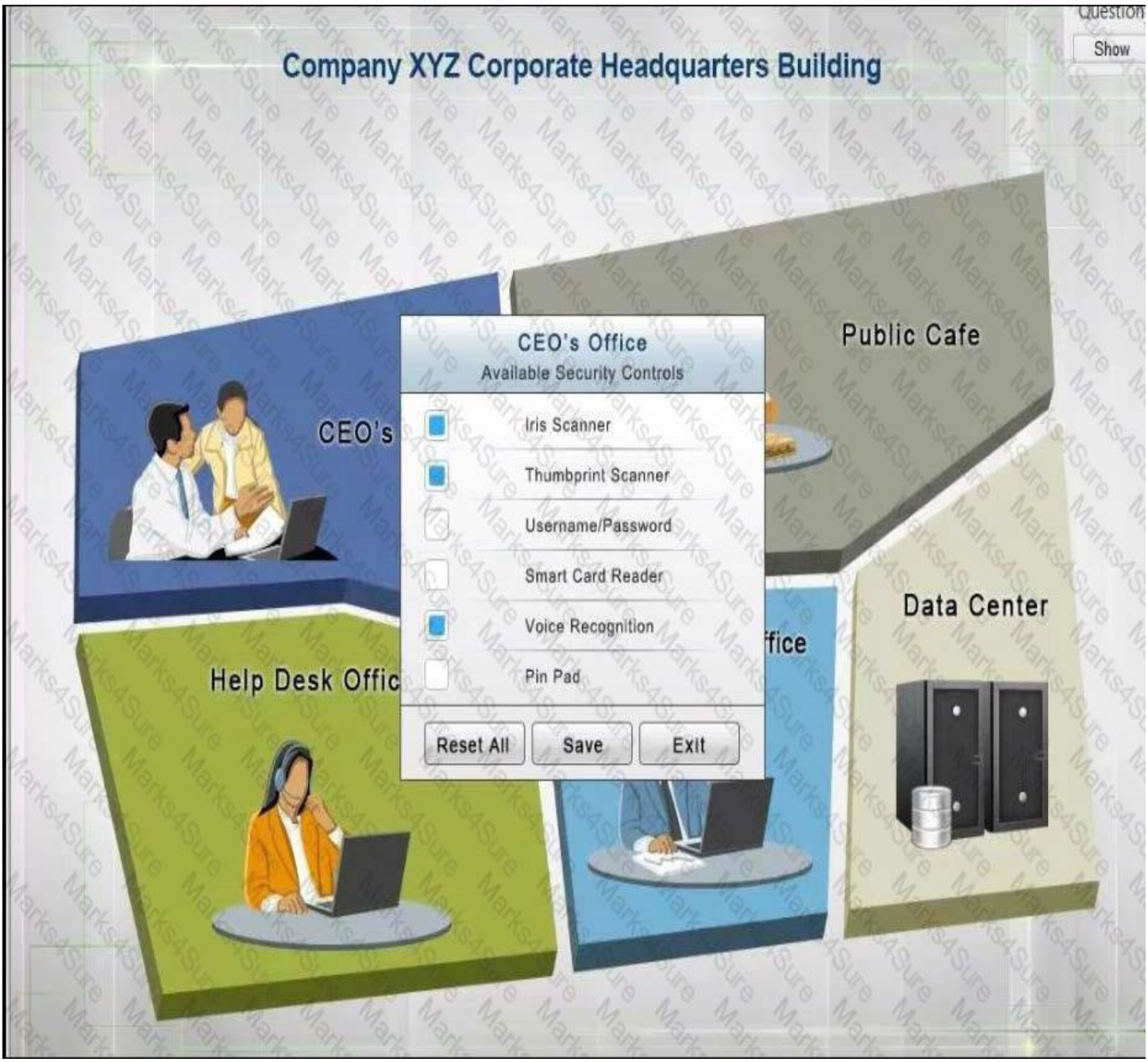
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.

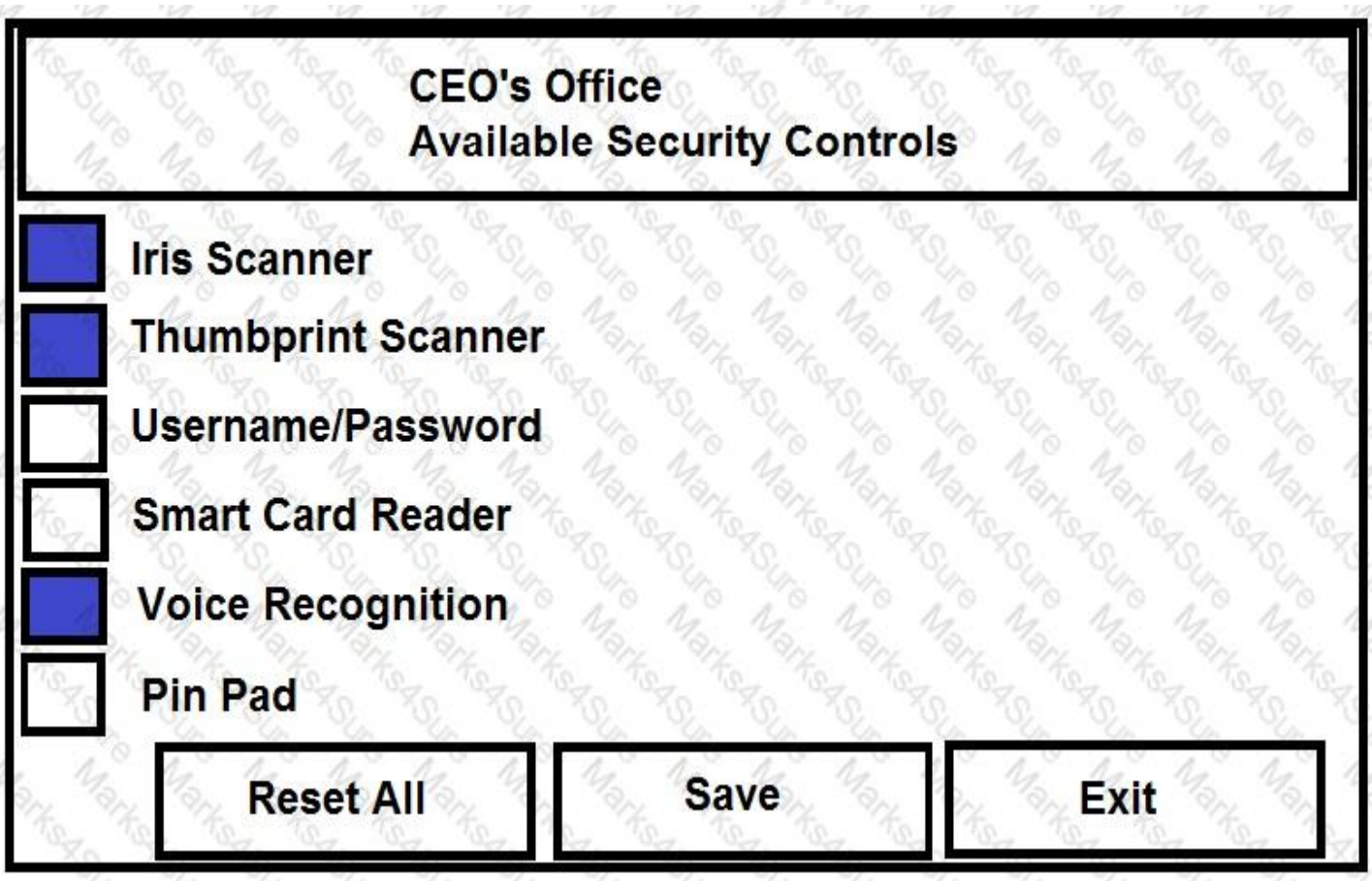


Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.


PII Processing Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Proximity Badge
Smart Card Reader
One Time Password Token
Pin Pad
Reset All
Save
Exit


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit



See the solution below.

Explanation

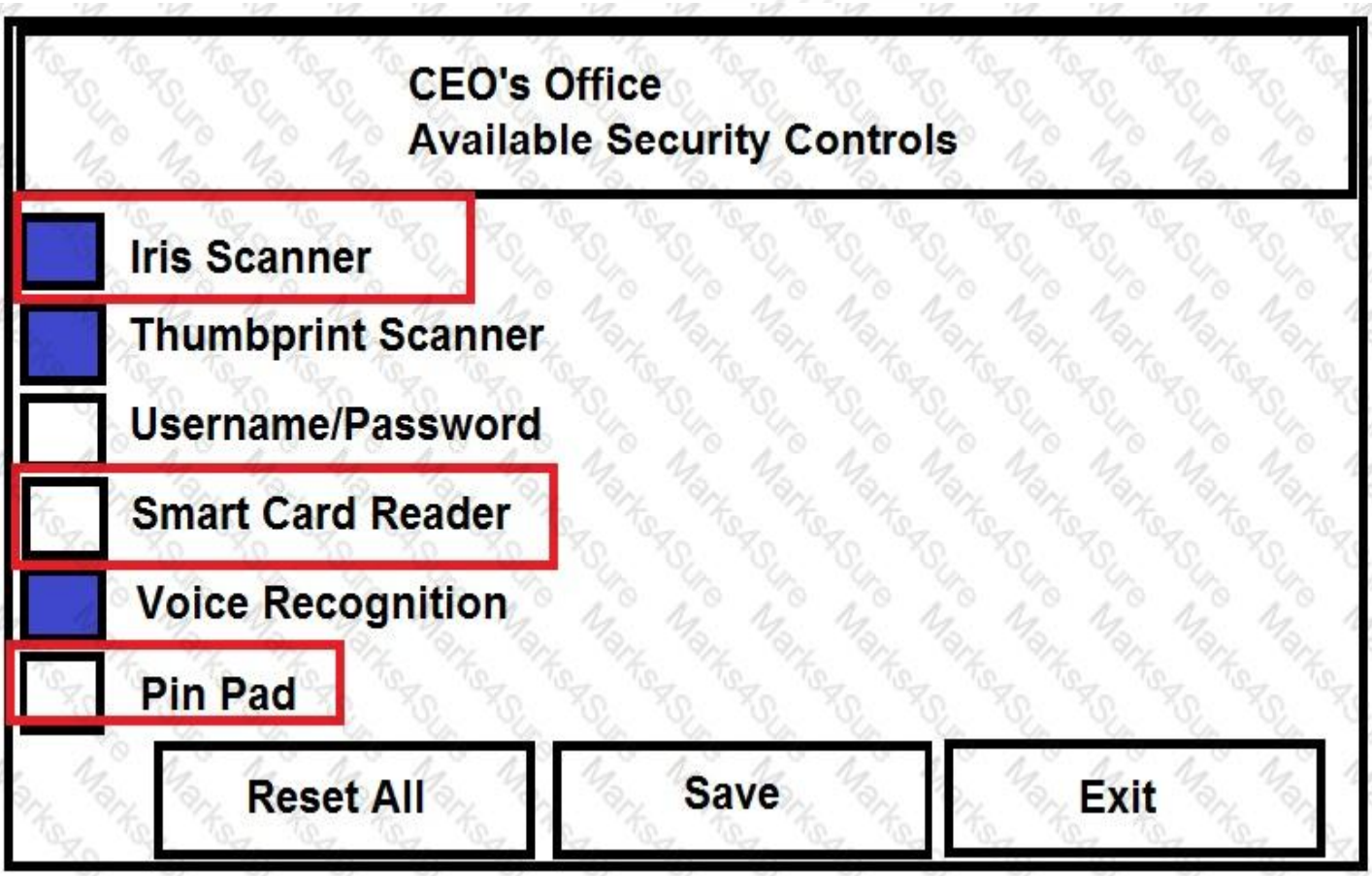
Solution as


PII Processing Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Proximity Badge
Smart Card Reader
One Time Password Token
Pin Pad
Reset All
Save
Exit


Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit


Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit


CEO's Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Username/Password
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

About Marks4sure.com

marks4sure.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- Sales: sales@marks4sure.com
- Feedback: feedback@marks4sure.com
- Support: support@marks4sure.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.