CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

A. Quarantining the compromised accounts and computers, only providing them with network access
B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
C. Isolating the compromised accounts and computers, cutting off all network and internet access.
D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 2
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

NEW QUESTION 3
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization’s vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

NEW QUESTION 4
An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

Answer: D

NEW QUESTION 5
Which of the following relets to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

Answer: A

NEW QUESTION 6
A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company’s data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

Answer: C

NEW QUESTION 7
A network administrator has been asked to design a solution to improve a company's security posture The administrator is given the following, requirements?
- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

Answer: D

NEW QUESTION 8
A security administrator currently spends a large amount of time on common security tasks, such aa report generation, phishing investigations, and user provisioning and deprovisioning This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

Answer: D

NEW QUESTION 9
A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

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

Answer: C

NEW QUESTION 10
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. 1s
D. setuid
E. nessus
F. nc

Answer: B

NEW QUESTION 10
An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 15
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. laaS
C. SaaS
D. PaaS

Answer: D

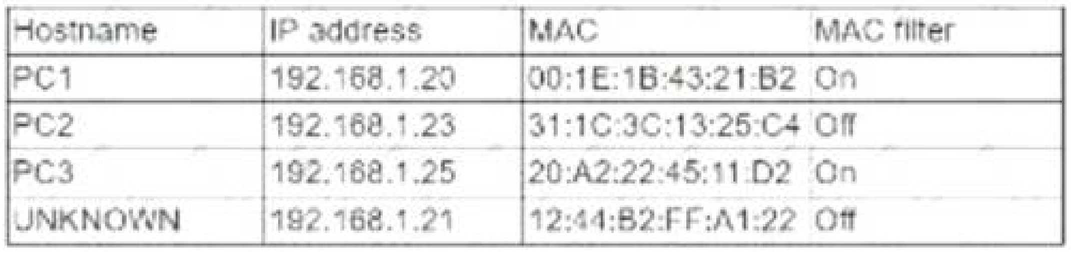
NEW QUESTION 20
An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization’s needs for a third factor?

A. Date of birth
B. Fingerprints
C. PIN
D. TPM

Answer: B

NEW QUESTION 24
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,

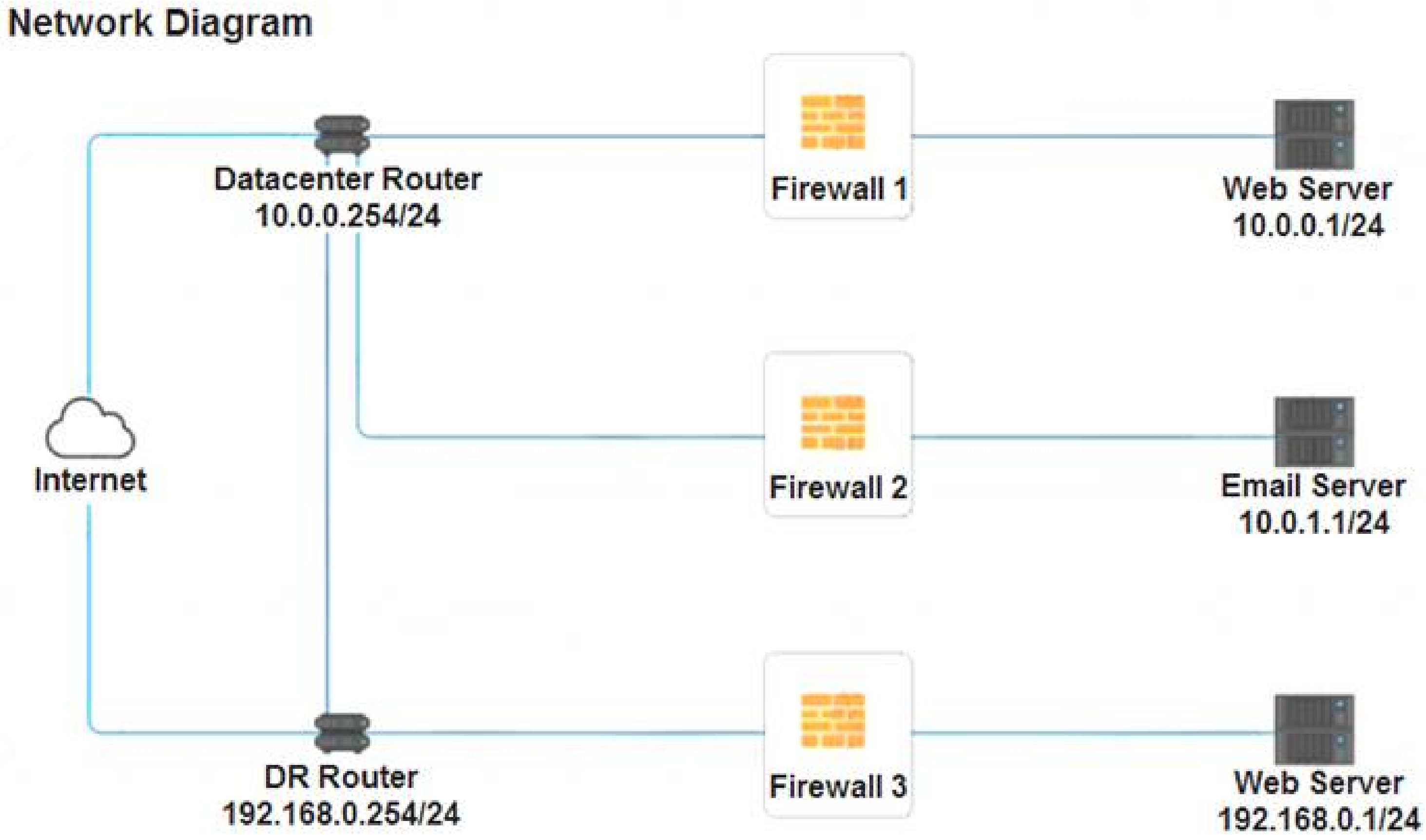
Answer: D

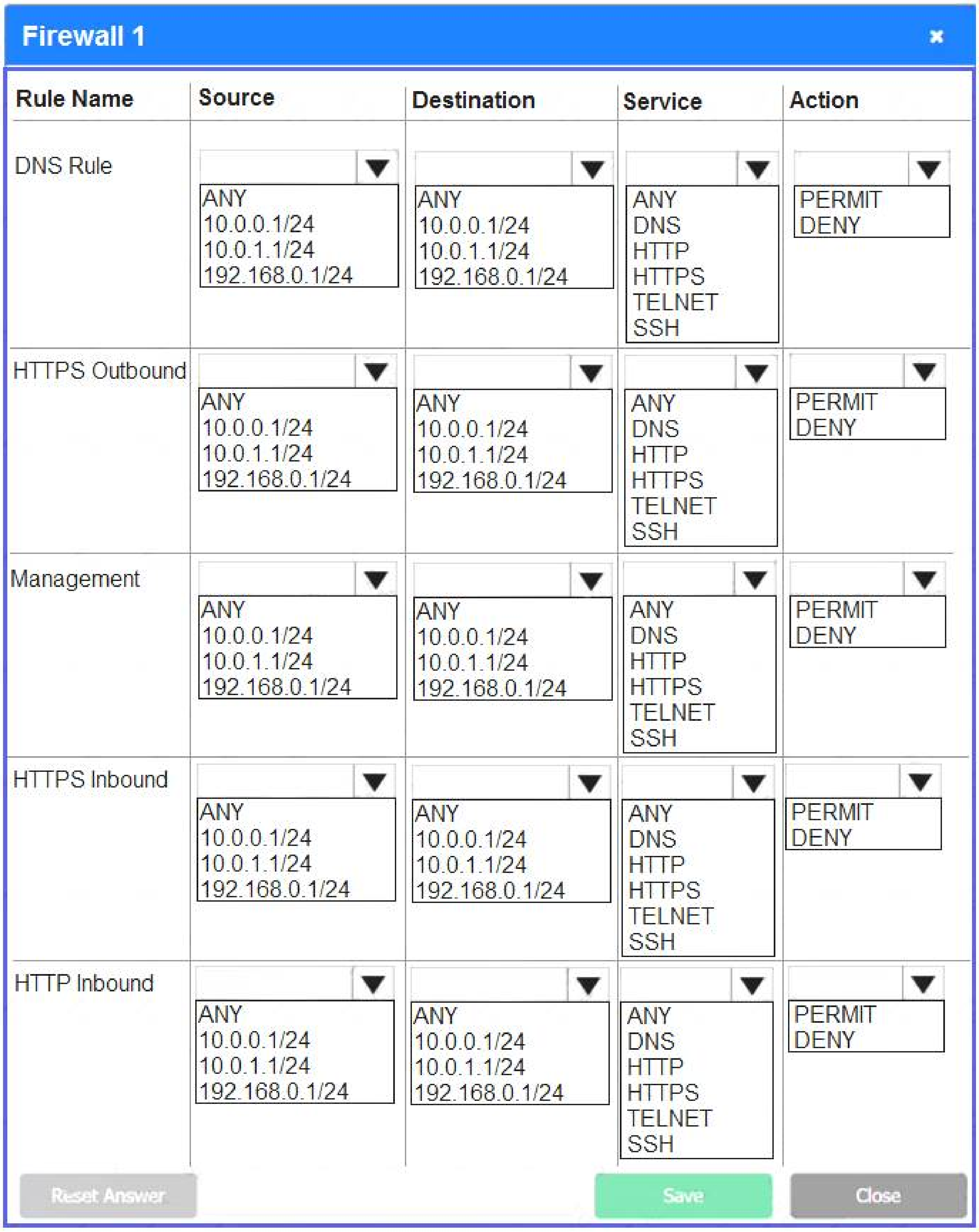
NEW QUESTION 26
A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A next-generation firewall

Answer: A

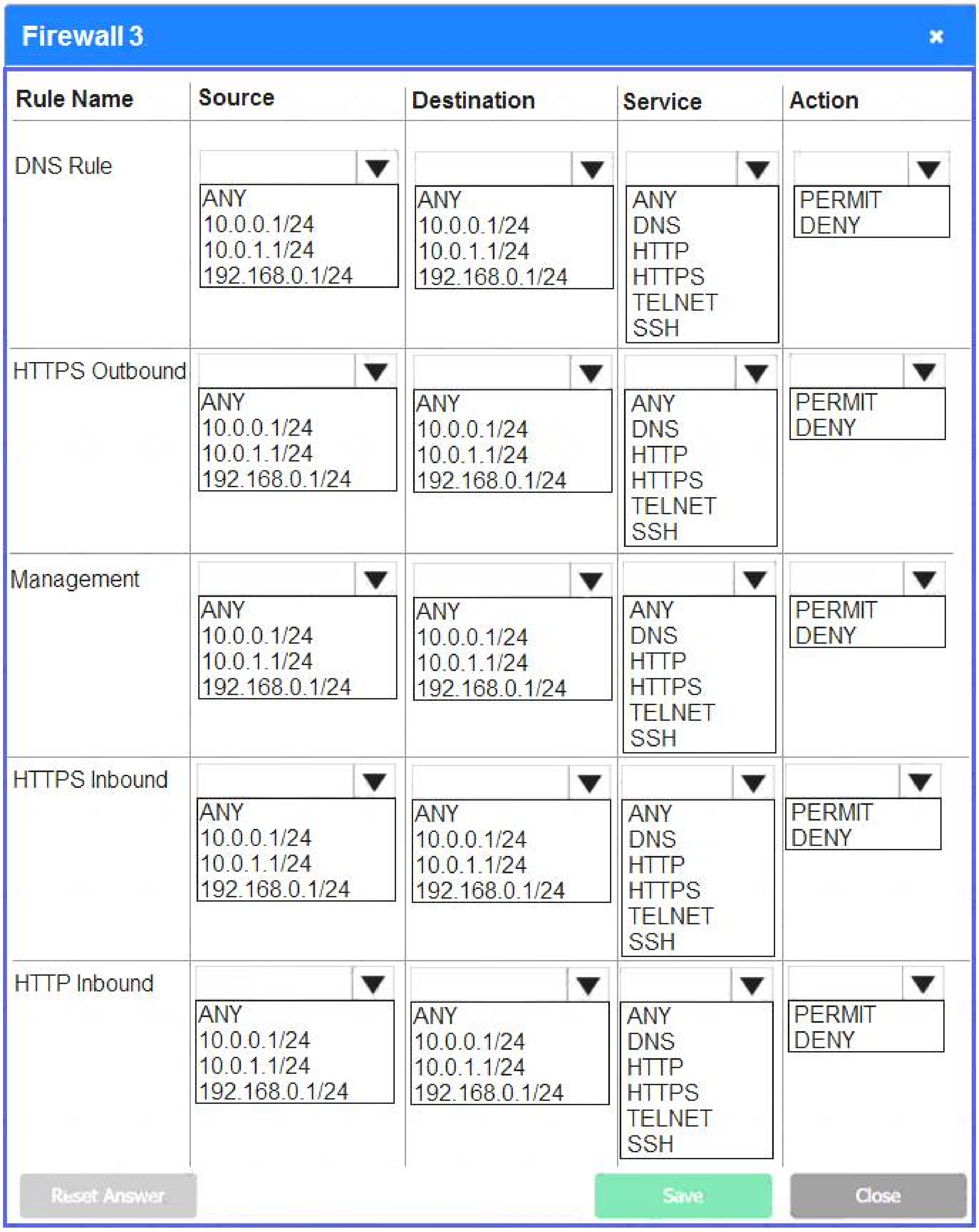
NEW QUESTION 31
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
Deny cleartext web traffic.
Ensure secure management protocols are used.
Resolve issues at the DR site.
The ruleset order cannot be modified due to outside constraints.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY



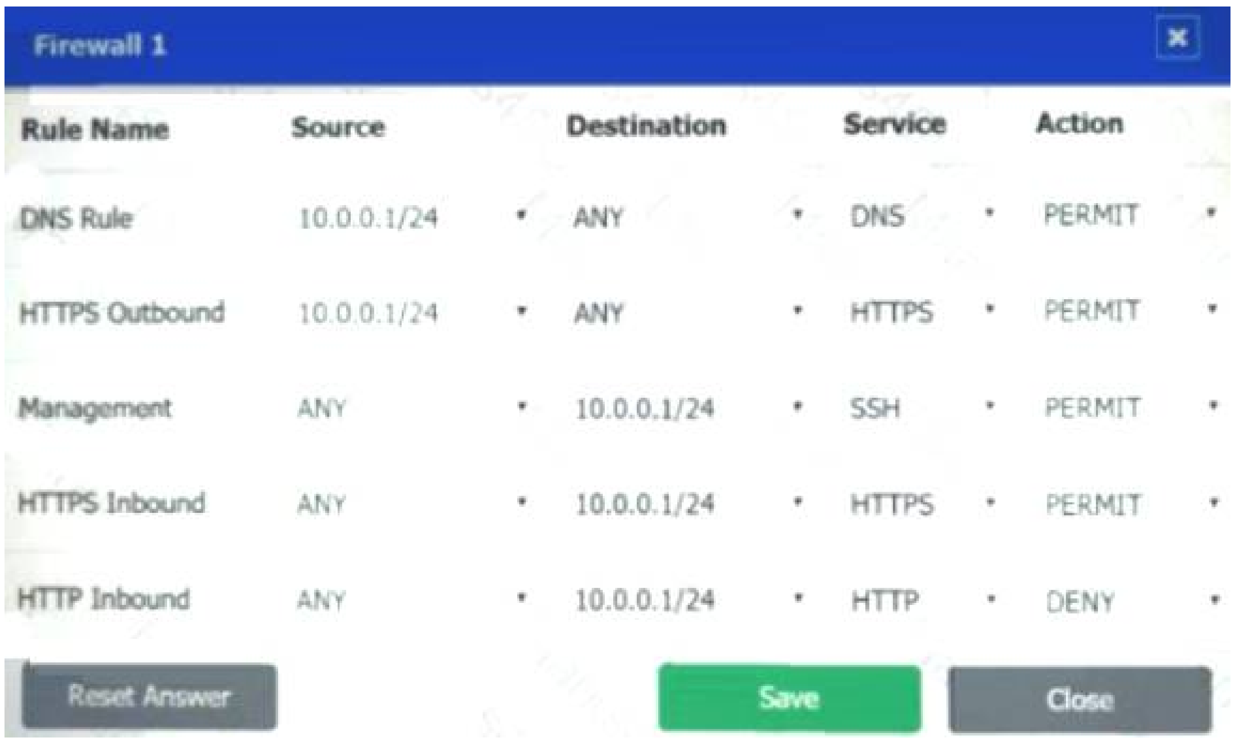
Firewall 3

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

A. Mastered
B. Not Mastered

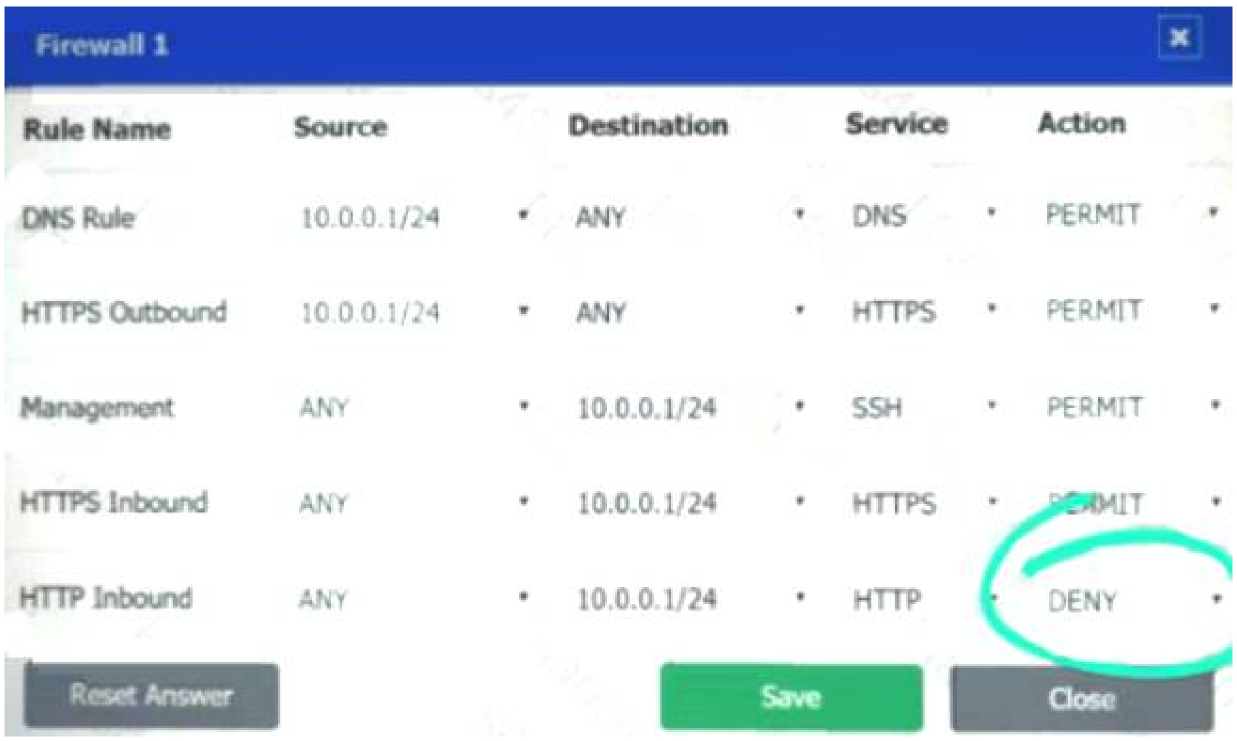
Answer: A

Explanation:
Firewall 1:



Firewall 1

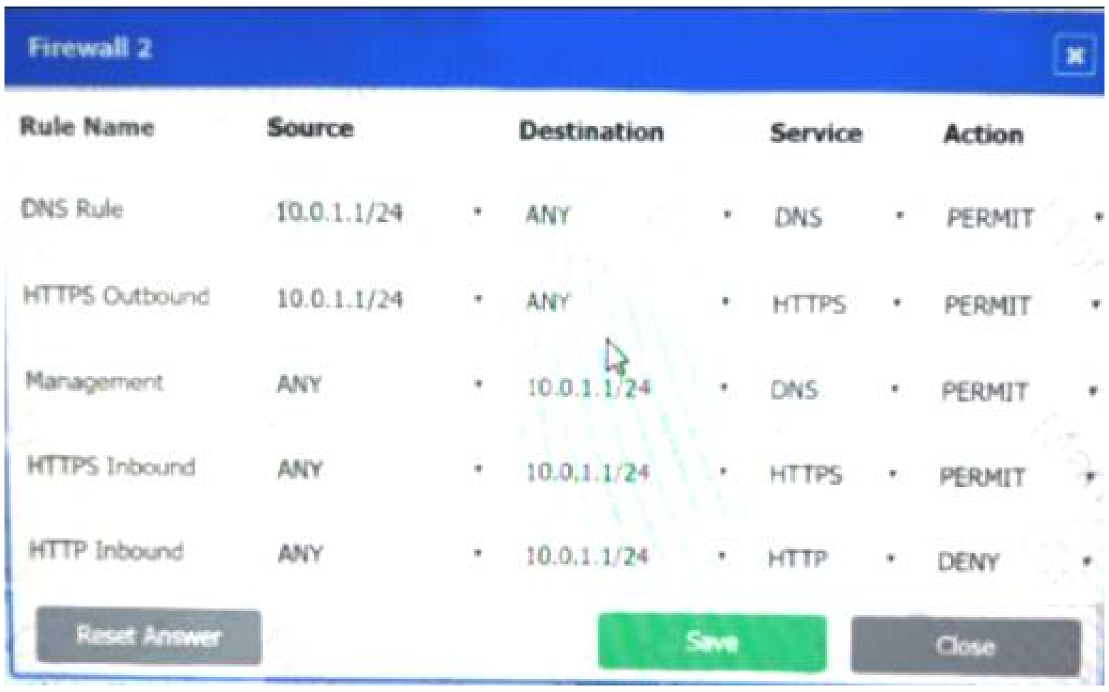
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY



Firewall 1

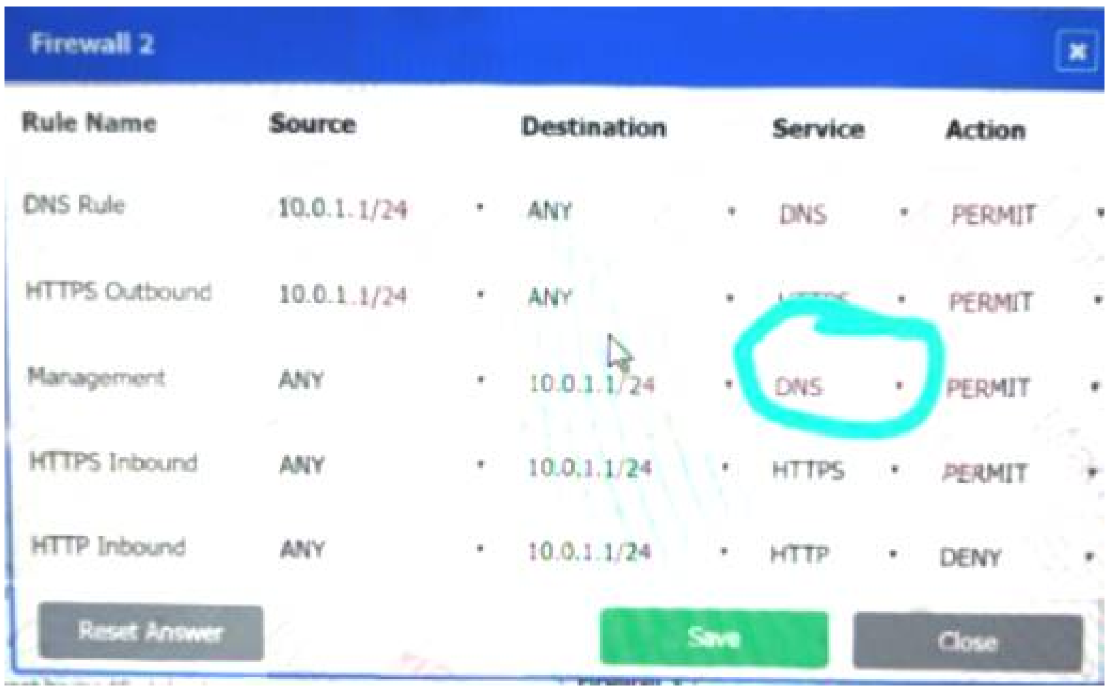
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY
Firewall 2:



Firewall 2

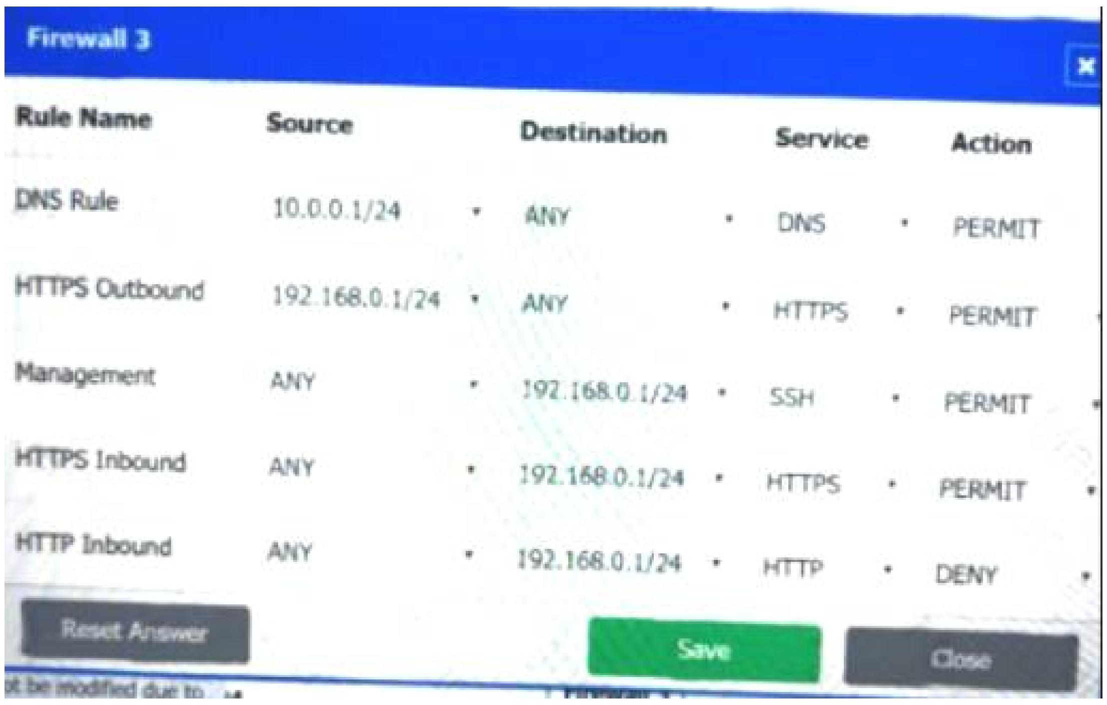
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY



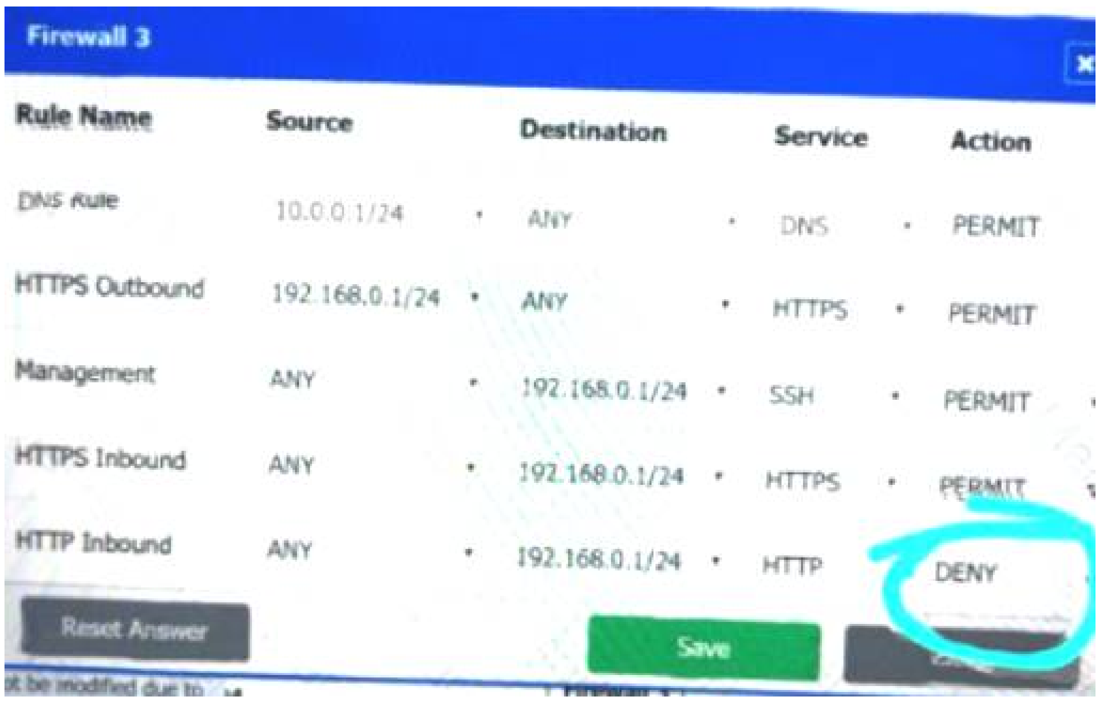
Firewall 2

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	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Firewall 3:



Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY



Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT
HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT
HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

NEW QUESTION 33
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: A

NEW QUESTION 38
A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan
B. Building a disaster recovery plan
C. Conducting a tabletop exercise
D. Running a simulation exercise

Answer: C

NEW QUESTION 40
A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lessons learned
D. Preparation

Answer: C

NEW QUESTION 42
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from

passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer: BD

NEW QUESTION 47
An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

Answer: C

NEW QUESTION 51
A cloud administrator is configuring five compute instances under the same subnet in a VPC Three instances are required to communicate with one another, and the other two must he logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

A. One security group
B. Two security groups
C. Three security groups
D. Five security groups

Answer: B

NEW QUESTION 55
A network engineer needs to build a solution that will allow guests at the company’s headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

A. Implement open PSK on the APs
B. Deploy a WAF
C. Configure WIPS on the APs
D. Install a captive portal

Answer: D

NEW QUESTION 56
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: AE

NEW QUESTION 57
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

NEW QUESTION 60
A user recently attended an exposition and received some digital promotional materials The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware

B. The user installed a cryptominer
C. The OS was corrupted
D. There was malicious code on the USB drive

Answer: D

NEW QUESTION 64
A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger
B. Metasploit
C. tcpdump
D. netstat

Answer: D

NEW QUESTION 69
The spread of misinformation surrounding the outbreak of a novel virus on election day ted to eligible voters choosing not to take the risk of going to the polls This is an example of:

A. prepending.
B. an influence campaign
C. a watering-hole attack
D. intimidation
E. information elicitation

Answer: D

NEW QUESTION 72
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs
B. The web server logs
C. The SIP traffic logs
D. The SNMP logs

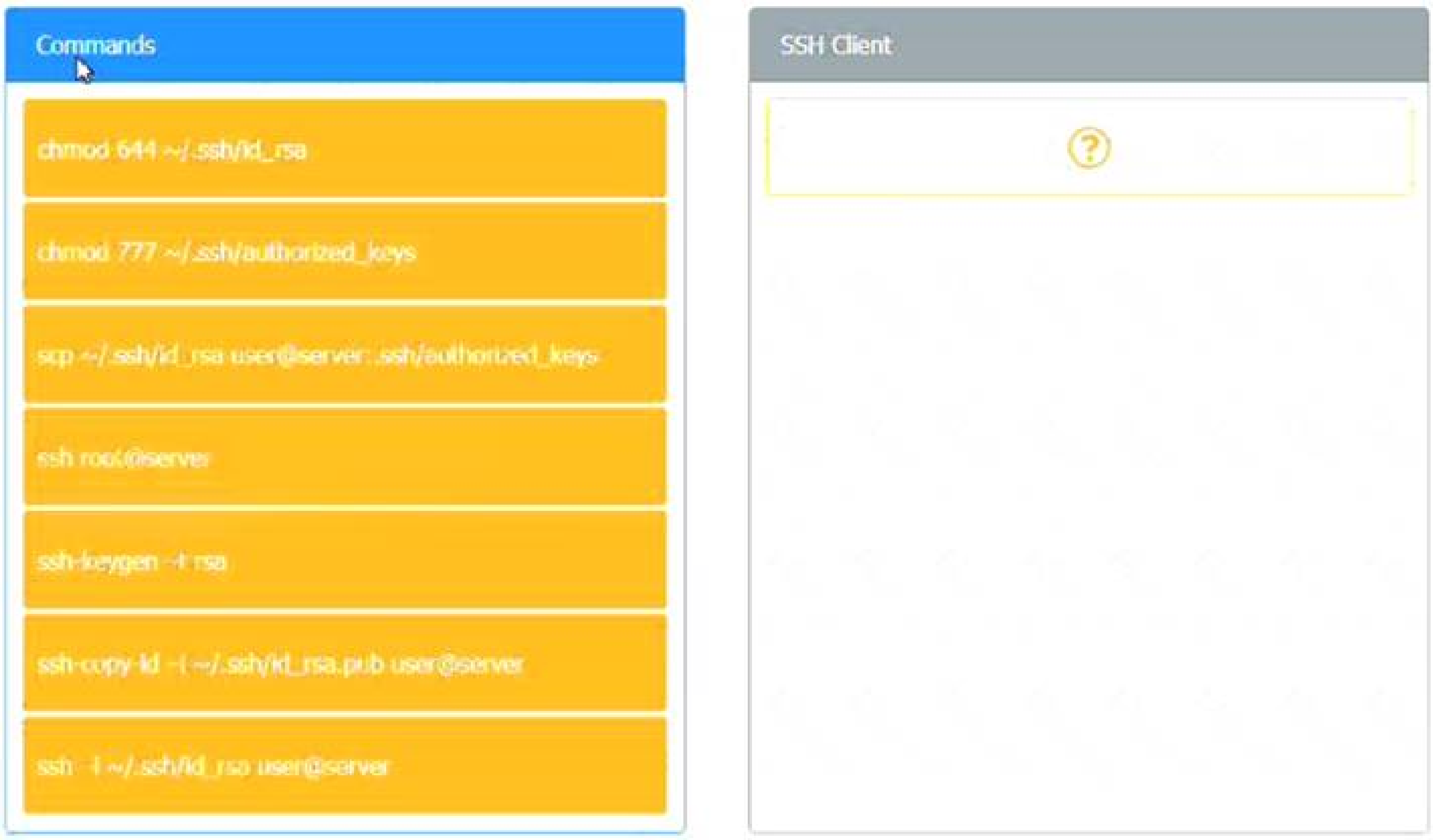
Answer: A

NEW QUESTION 73
A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

A. # iptables -t mangle -X
B. # iptables -F
C. # iptables -Z
D. # iptables -P INPUT -j DROP

Answer: D

NEW QUESTION 77
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

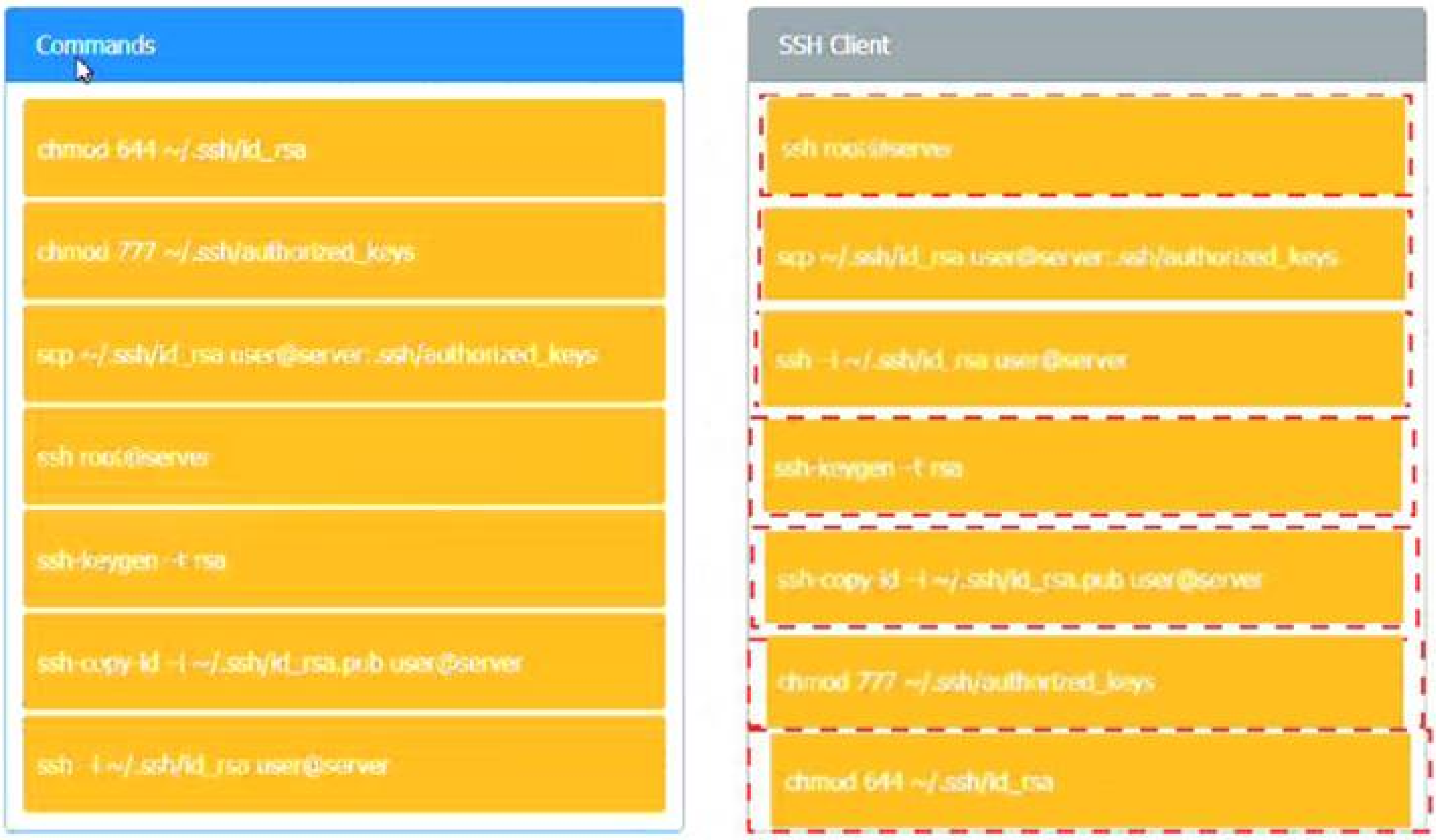
SSH Client

?

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

ssh root@server

scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys

ssh -i ~/.ssh/id_rsa user@server

ssh-keygen -t rsa

ssh-copy-id -i ~/.ssh/id_rsa.pub user@server

chmod 777 ~/.ssh/authorized_keys

chmod 644 ~/.ssh/id_rsa

NEW QUESTION 82

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers
B. State actors
C. Script kiddies
D. Advanced persistent threats

Answer: B

NEW QUESTION 83

A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

A. OAuth
B. TACACS+
C. SAML
D. RADIUS

Answer: D

NEW QUESTION 84
A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:
Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Answer: C

NEW QUESTION 89
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Answer: B

NEW QUESTION 94
Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

Answer: B

NEW QUESTION 97
A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

A. Unsecme protocols
B. Default settings
C. Open permissions
D. Weak encryption

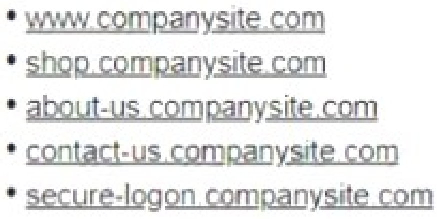
Answer: D

NEW QUESTION 98
Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is
configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

A. WPA3
B. AES
C. RADIUS
D. WPS

Answer: D

NEW QUESTION 100
A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:



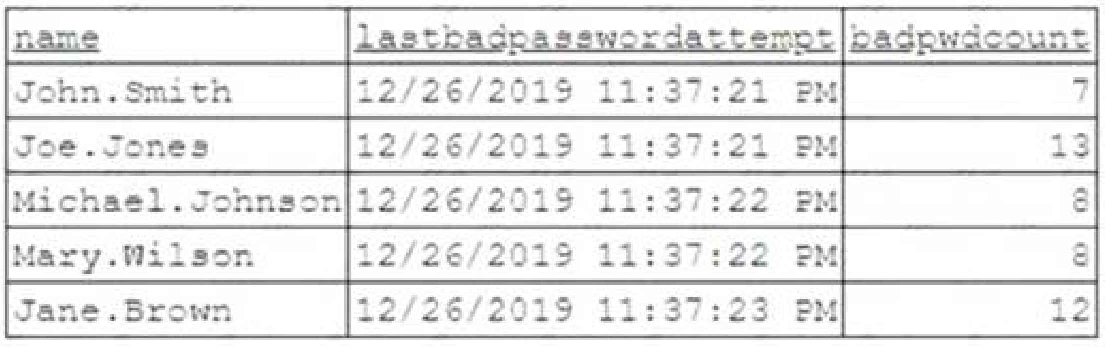
- www.companysite.com
- shop.companysite.com
- about-us.companysite.com
- contact-us.companysite.com
- secure-logon.companysite.com

Which of the following should the company use to secure its website rf the company is concerned with convenience and cost?

A. A self-signed certificate
B. A root certificate
C. A code-signing certificate
D. A wildcard certificate
E. An extended validation certificate

Answer: B

NEW QUESTION 101
A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:
To better understand what is going on, the analyst runs a command and receives the following output:



name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

Answer: D

NEW QUESTION 103
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 to ensure it 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 daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch ail systems and applications.
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and perform user application hardening

Answer: A

NEW QUESTION 104
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: BE

NEW QUESTION 109
A large financial services firm recently released information regarding a security bfeach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gam access?

A. A bot
B. A fileless virus
C. A logic bomb
D. A RAT

Answer: D

NEW QUESTION 113
A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

Answer: D

NEW QUESTION 114
Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC

B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 117
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 m 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: A

NEW QUESTION 120
Which of the following describes the ability of code to target a hypervisor from inside

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

Answer: B

NEW QUESTION 125
Which of the following algorithms has the SMALLEST key size?

A. DES
B. Twofish
C. RSA
D. AES

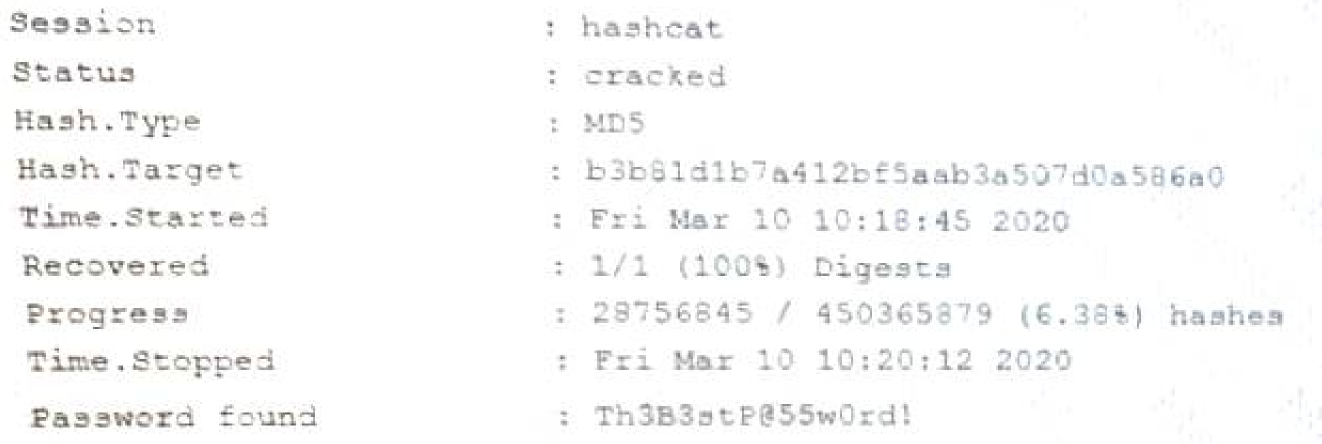
Answer: B

NEW QUESTION 130
A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identity the weak spots.
B. Use a packet analyzer to Investigate the NetFlow traffic.
C. Check the SIEM to review the correlated logs.
D. Require access to the routers to view current sessions.

Answer: C

NEW QUESTION 135
An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:



```
Session                    : hashcat
Status                     : cracked
Hash.Type                  : MD5
Hash.Target                : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started               : Fri Mar 10 10:18:45 2020
Recovered                  : 1/1 (100%) Digests
Progress                   : 28756845 / 450365879 (6.38%) hashes
Time.Stopped               : Fri Mar 10 10:20:12 2020
Password found             : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary
B. Pass-the-hash
C. Brute-force
D. Password spraying

Answer: A

NEW QUESTION 139
A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC
B. Reverse proxy
C. VPN concentrator
D. PKI
E. Active Directory
F. RADIUS

Answer: EF

NEW QUESTION 142
The process of passively gathering information prior to launching a cyberattack is called:

A. tailgating
B. reconnaissance
C. pharming
D. prepending

Answer: B

NEW QUESTION 146
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

Answer: C

NEW QUESTION 149
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 153
An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack
B. A watering-hole attack
C. Typo squatting
D. A phishing attack

Answer: B

NEW QUESTION 154
A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan Types would produce the BEST vulnerability scan report?

A. Port
B. Intrusive
C. Host discovery
D. Credentialed

Answer: D

NEW QUESTION 157
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The Oss are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

Answer: D

NEW QUESTION 162
An organization just experienced a major cyberattack modem. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

Answer: D

NEW QUESTION 166
A cybersecurity department purchased o new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

A. Randomize the shared credentials
B. Use only guest accounts to connect.
C. Use SSH keys and remove generic passwords
D. Remove all user accounts.

Answer: C

NEW QUESTION 170
Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Answer: B

NEW QUESTION 174
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each regio
D. limit their logon times, and alert on risky logins
E. Create a guest account for each regio
F. remember the last ten passwords, and block password reuse

Answer: C

NEW QUESTION 177
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

A. The S/MME plug-in is not enabled.
B. The SLL certificate has expired.
C. Secure IMAP was not implemented
D. POP3S is not supported.

Answer: A

NEW QUESTION 180
A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

A. Automated information sharing
B. Open-source intelligence
C. The dark web
D. Vulnerability databases

Answer: C

NEW QUESTION 185
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information
B. Encrypting the credit card information in transit.
C. Hashing the credit card numbers upon entry.
D. Tokenizing the credit cards in the database

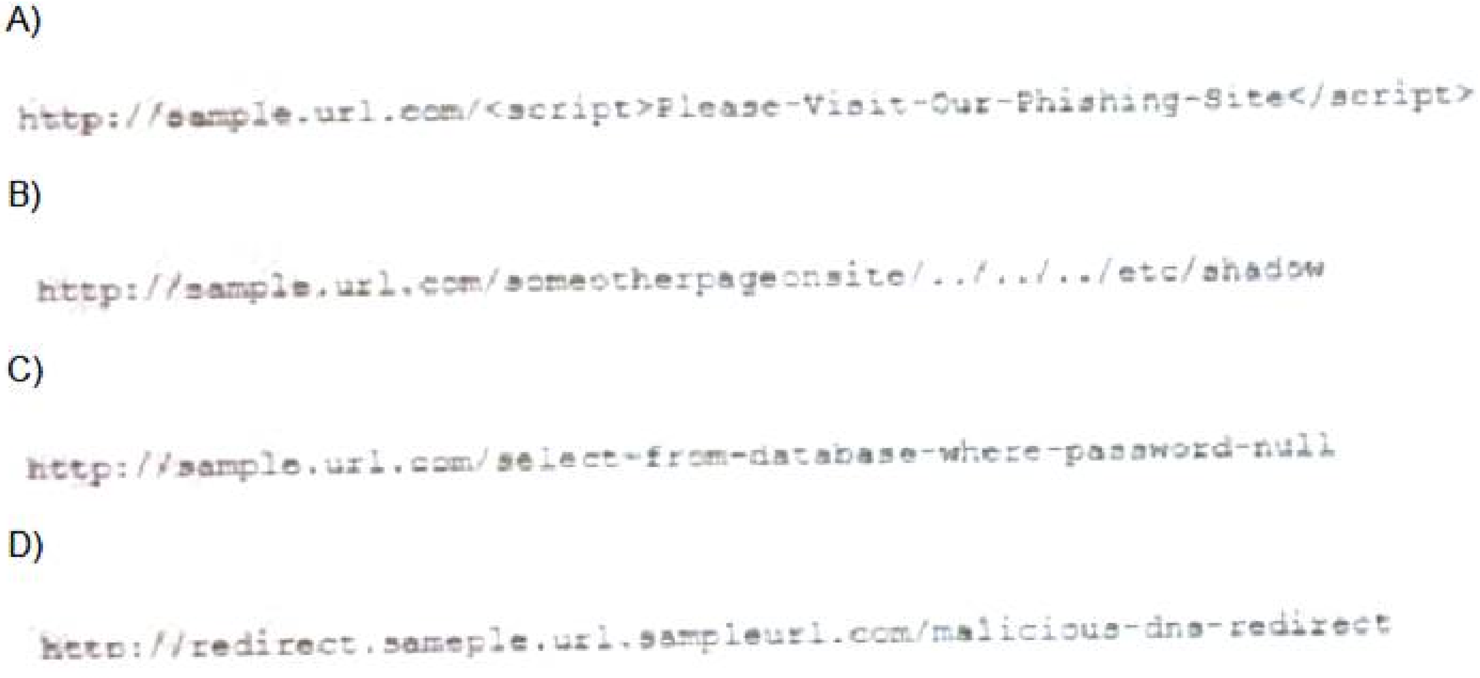
Answer: C

NEW QUESTION 190
An organization is concerned that is 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 comptia, org –p 80
B. Nc -1 –v comptia, org –p 80
C. nmp comptia, org –p 80 –aV
D. nslookup –port=80 comtia.org

Answer: C

NEW QUESTION 194
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?



A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

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

Answer: B

NEW QUESTION 195
A security analyst has received an alert about being sent via email. The analyst’s Chief information Security Officer (CISO) has made it clear that PII must be handle with extreme care From which of the following did the alert MOST likely originate?

A. S/MIME
B. DLP
C. IMAP
D. HIDS

Answer: B

NEW QUESTION 196
Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

A. Testing security systems and processes regularly
B. Installing and maintaining a web proxy to protect cardholder data
C. Assigning a unique ID to each person with computer access
D. Encrypting transmission of cardholder data across private networks
E. Benchmarking security awareness training for contractors
F. Using vendor-supplied default passwords for system passwords

Answer: BD

NEW QUESTION 200
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO’s concerns?

A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of system if the provider goes offline.

Answer: D

NEW QUESTION 204
A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications.
After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

A. DLP
B. SWG
C. CASB
D. Virtual network segmentation
E. Container security

Answer: A

NEW QUESTION 208
In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

A. Identification
B. Preparation
C. Eradiction
D. Recovery
E. Containment

Answer: E

NEW QUESTION 212
A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you are
E. Something you are
F. Something you can do

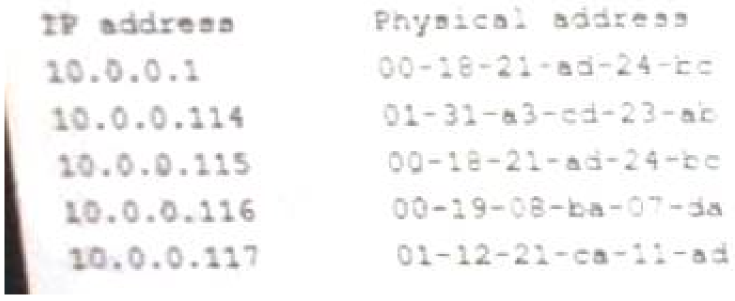
Answer: BE

NEW QUESTION 216
Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to be kept for a minimum of 30 days
C. Integration of threat intelligence in the company's AV
D. A data-breach clause requiring disclosure of significant data loss

Answer: A

NEW QUESTION 221
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet, While reviewing logs and tool output, the analyst sees the following:



```
IP address        Physical address
10.0.0.1          00-18-21-ad-24-bc
10.0.0.114        01-31-a3-cd-23-ab
10.0.0.115        00-18-21-ad-24-bc
10.0.0.116        00-19-08-ba-07-da
10.0.0.117        01-12-21-ca-11-ad
```

Which of the following attacks has occurred?

A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Answer: E

NEW QUESTION 224
A company recently experienced an attack in which a malicious actor was able to exfiltrate data by cracking stolen passwords, using a rainbow table the sensitive

data. Which of the following should a security engineer do to prevent such an attack in the future?

A. Use password hashing.
B. Enforce password complexity.
C. Implement password salting.
D. Disable password reuse.

Answer: D

NEW QUESTION 228
A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks When of the following should the engineer implement?

A. An air gap
B. A hot site
C. AVLAN
D. A screened subnet

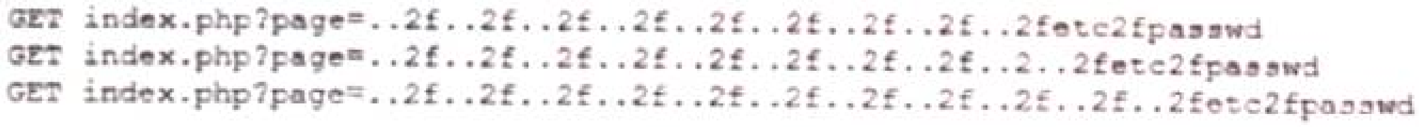
Answer: D

NEW QUESTION 233
A network administrator would like to configure a site-to-site VPN utilizing iPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

A. AH
B. EDR
C. ESP
D. DNSSEC

Answer: C

NEW QUESTION 235
A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:



```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

A. Directory traversal
B. SQL injection
C. API
D. Request forgery

Answer: D

NEW QUESTION 238
Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

A. The employee's physical access card was cloned.
B. The employee is colluding with human resources
C. The employee's biometrics were harvested
D. A criminal used lock picking tools to open the door.

Answer: A

NEW QUESTION 242
The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the worker's PC. Which of the following would be BEST to help prevent this type of attack in the future?

A. Data loss prevention
B. Segmentation
C. Application whitelisting
D. Quarantine

Answer: C

NEW QUESTION 244
A workwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location

B. Impossible travel time
C. Geolocation
D. Geofencing

Answer: D

NEW QUESTION 247
A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:
- Mobile device OSs must be patched up to the latest release
- A screen lock must be enabled (passcode or biometric)
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

A. Containerization
B. Storage segmentation
C. Posturing
D. Remote wipe
E. Full-device encryption
F. Geofencing

Answer: DE

NEW QUESTION 252
Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

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

Answer: A

NEW QUESTION 256
After consulting with the Chief Risk Officer (CRO). a manager decides to acquire cybersecurity insurance for the company Which of the following risk management strategies is the manager adopting?

A. Risk acceptance
B. Risk avoidance
C. Risk transference
D. Risk mitigation

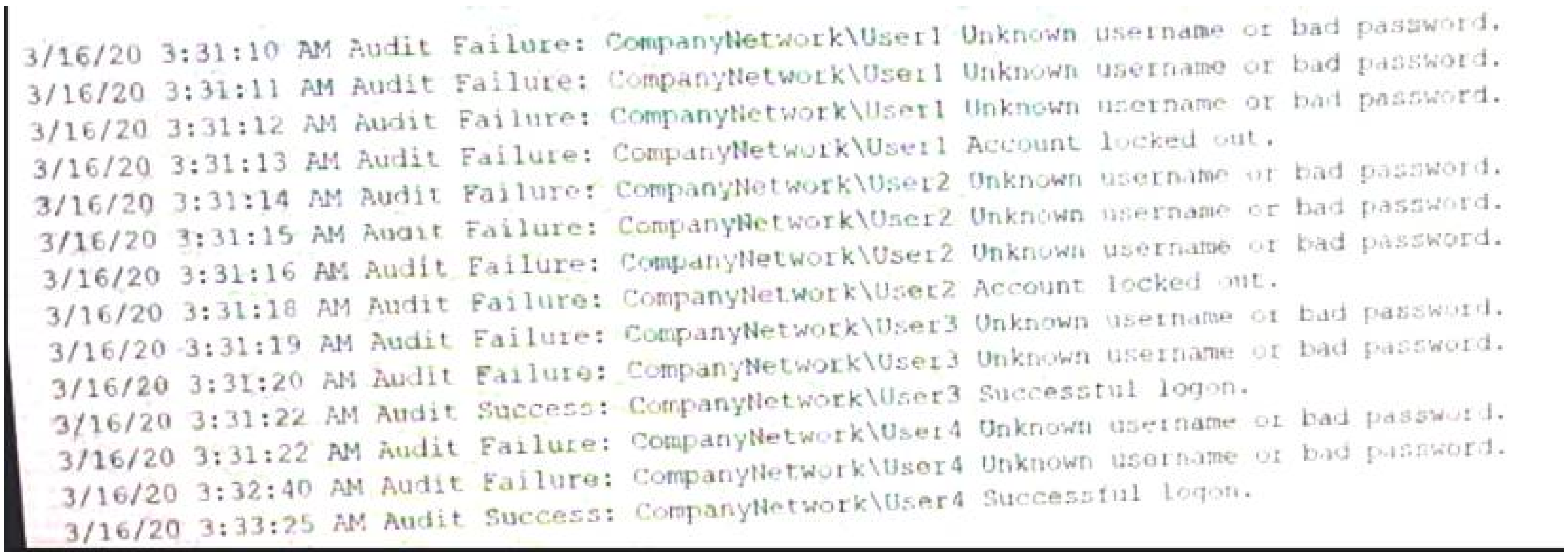
Answer: C

NEW QUESTION 257
Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

Answer: DF

NEW QUESTION 261
A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute-force

Answer: D

NEW QUESTION 265
An organization blocks user access to command-line interpreters but hackers still managed to invoke the interpreters using native administrative tools Which of the following should the security team do to prevent this from Happening in the future?

A. Implement HIPS to block Inbound and outbound SMB ports 139 and 445.
B. Trigger a SIEM alert whenever the native OS tools are executed by the user
C. Disable the built-in OS utilities as long as they are not needed for functionality.
D. Configure the AV to quarantine the native OS tools whenever they are executed

Answer: C

NEW QUESTION 267
A security administrator needs to inspect in-transit files on the enterprise network to search for Pll, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution
B. EDR solution
C. HIPS software solution
D. Network DLP solution

Answer: D

NEW QUESTION 269
A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. OSINT
B. SIEM
C. CVSS
D. CVE

Answer: D

NEW QUESTION 271
An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

Answer: A

NEW QUESTION 273
A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

NEW QUESTION 278
A user contacts the help desk to report the following:
 Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
 The user was able to access the Internet but had trouble accessing the department share until the next day.
 The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

Answer: A

NEW QUESTION 282
A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs
B. Common Vulnerabilities and Exposures
C. Static code analysis
D. Non-credentialed scans

Answer: C

NEW QUESTION 284
Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Answer: B

NEW QUESTION 288
A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

A. HIDS
B. UEBA
C. CASB
D. VPC

Answer: C

NEW QUESTION 291
A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

Answer: B

NEW QUESTION 295
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which of the following configuration should an analyst enable to improve security? (Select Two)

A. RADIUS
B. PEAP
C. WPS
D. WEP-TKIP
E. SSL
F. WPA2-PSK

Answer: DF

NEW QUESTION 297

......