CompTIA.SY0-601.v2025-01-07.q105

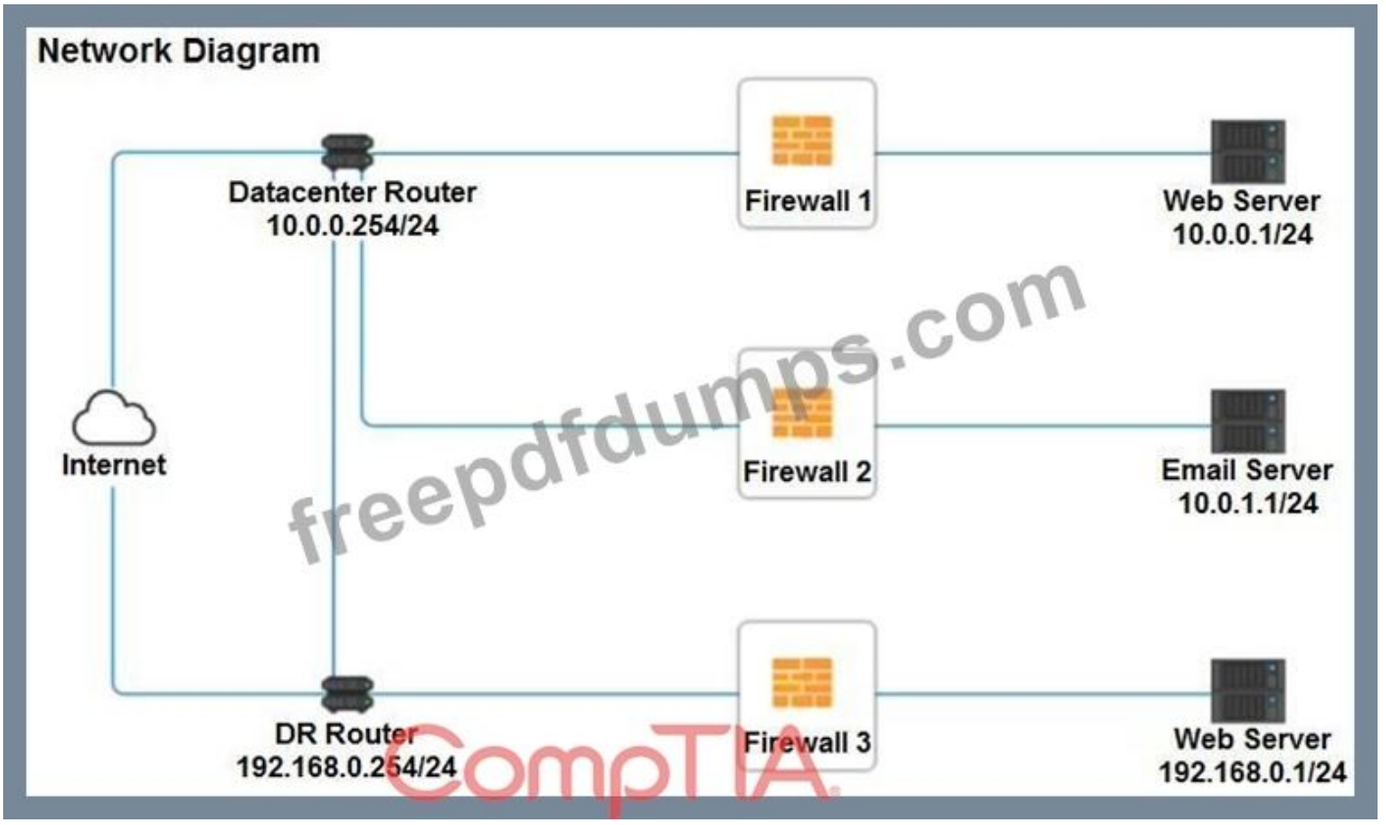
Exam Code:	SY0-601
Exam Name:	CompTIA Security+ Exam
Certification Provider:	CompTIA
Free Question Number:	105
Version:	v2025-01-07
# of views:	622
# of Questions views:	1050
https://www.freepdfdumps.com/CompTIA.SY0-601.v2025-01-07.q105.html	

NEW QUESTION: 1
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?
A. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan
Answer: B (LEAVE A REPLY)
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.
An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION: 2
During an investigation, events from two affected servers in the same subnetwork occurred at the same time:
Server 1: 192.168.10.1 [01/Apr/2021:06:00:00 PST] SAN access denied for user 'admin' Server 2: 192.168.10.6 [01/Apr/2021:06:01:01 CST] SAN access successful for user 'admin Which of the following should be consistently configured to prevent the issue seen in the logs?
A. TOTP
B. MFA

C. NTP
D. Geolocation
Answer: C (LEAVE A REPLY)

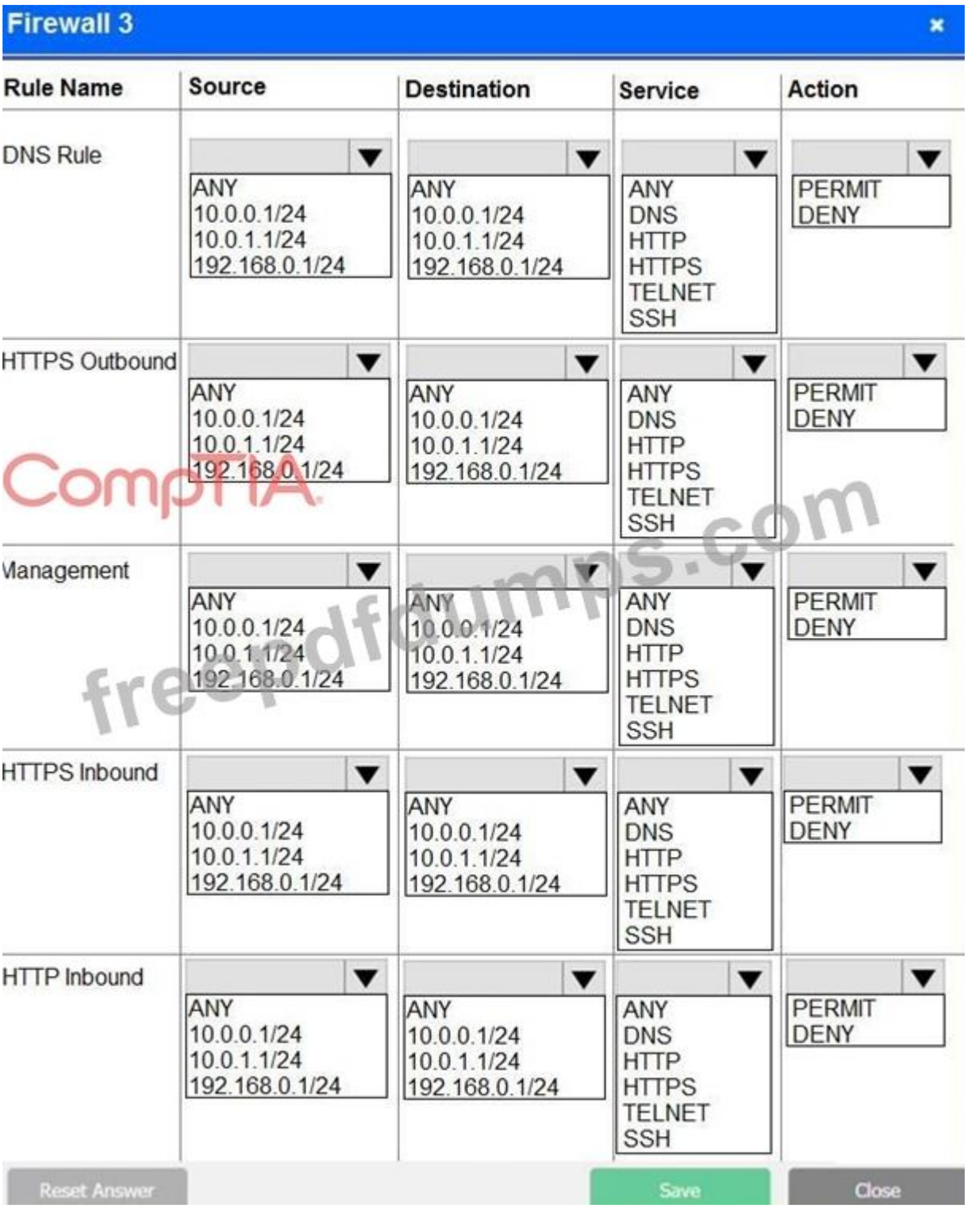
NEW QUESTION: 3
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
* Deny cleartext web traffic.
* Ensure secure management protocols are used. Please Resolve issues at the 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 2

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

Reset Answer | Save | Close



Answer:

See explanation below.

Explanation

Firewall 1:

DNS Rule - ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound - 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT

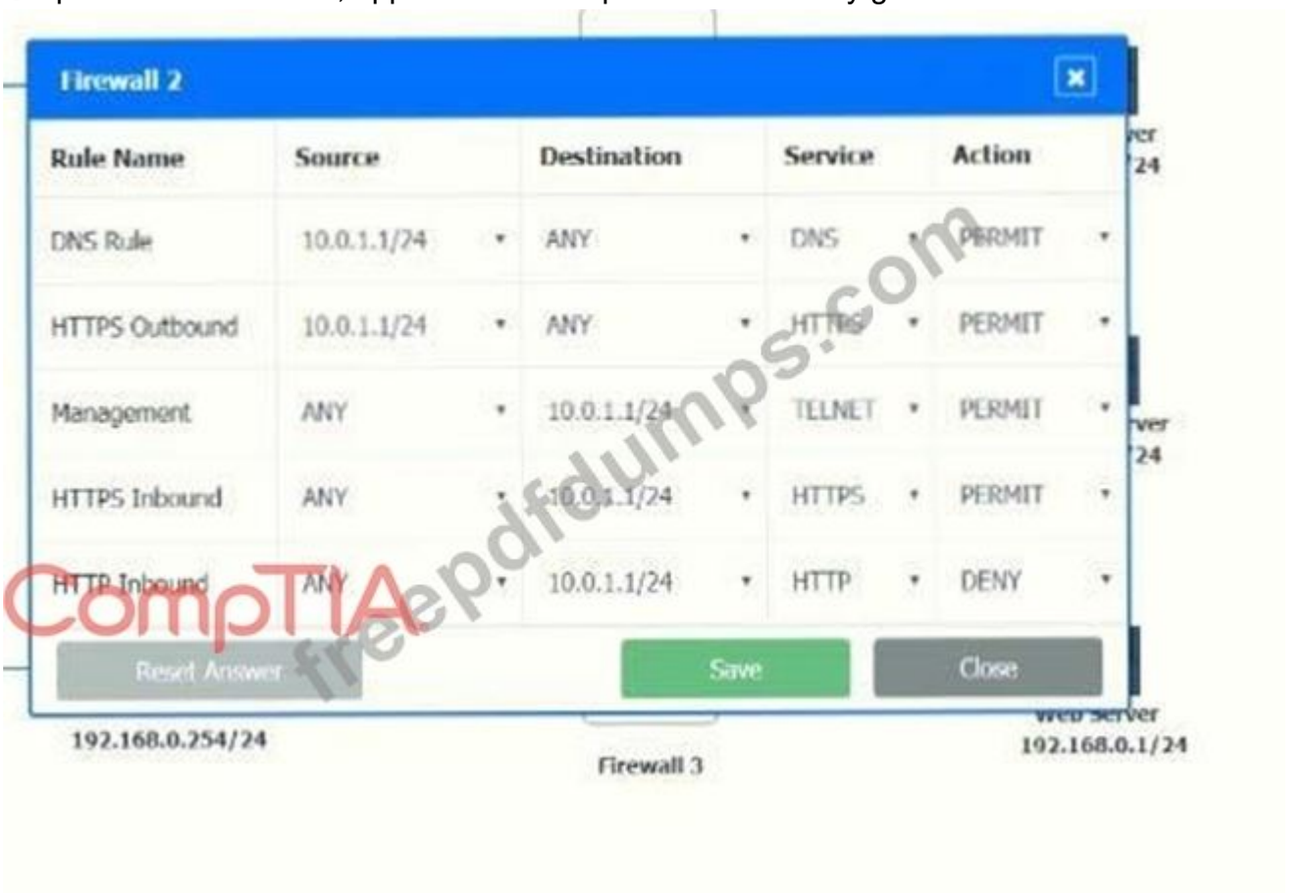
Management - ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound - ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound - ANY --> ANY --> HTTP --> DENY

Firewall 2: No changes should be made to this firewall

Graphical user interface, application Description automatically generated



Firewall 3:

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

Graphical user interface, application Description automatically generated

NEW QUESTION: 4
A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?
A. Update the base container image and redeploy the environment.
B. Include the containers in the regular patching schedule for servers
C. Patch each running container individually and test the application
D. Update the host in which the containers are running
Answer: C (LEAVE A REPLY)
Explanation
A container image vulnerability is a security risk that is embedded inside a container image. While vulnerable images themselves don't pose an active threat, if containers are created based on a vulnerable image, the containers will introduce the vulnerability to a live environment.

NEW QUESTION: 5
The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:
* Minimal interruption to the end user
* Mutual certificate validation
Which of the following authentication protocols would meet these requirements?
A. EAP-FAST
B. PSK

C. EAP-TTLS
D. EAP-TLS
Answer: (SHOW ANSWER)
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

NEW QUESTION: 6
Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?
A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold
Answer: (SHOW ANSWER)
Order of volatility is the order in which a forensic specialist should collect evidence based on how quickly the data can be lost or altered. The most volatile data, such as CPU registers and cache, should be collected first, followed by less volatile data, such as disk drives and archival media. Order of volatility helps preserve the integrity and validity of the evidence and prevent data loss or corruption123 References: CompTIA Security+ SY0-601 Certification Study Guide, Chapter 11: Explaining Digital Forensics Concepts, page 494; Order of Volatility - Computer Forensics Recruiter; Order of Volatility - CompTIA Security+ SY0-401: 2.4; CFR and Order of Volatility - Get Certified Get Ahead

NEW QUESTION: 7
Local guidelines require that all information systems meet a minimum security baseline to be compliant Which of the following can security administrators use to assess their system configurations against the baseline?
A. SOAR playbook
B. Security control matrix
C. Risk management framework
D. Benchmarks
Answer: (SHOW ANSWER)
Benchmarks are predefined sets of configuration standards or best practices for securing information systems and networks. Benchmarks can be used to assess system configurations against the minimum security baseline required by local guidelines or industry regulations. Benchmarks can also provide guidance on how to remediate any deviations or vulnerabilities

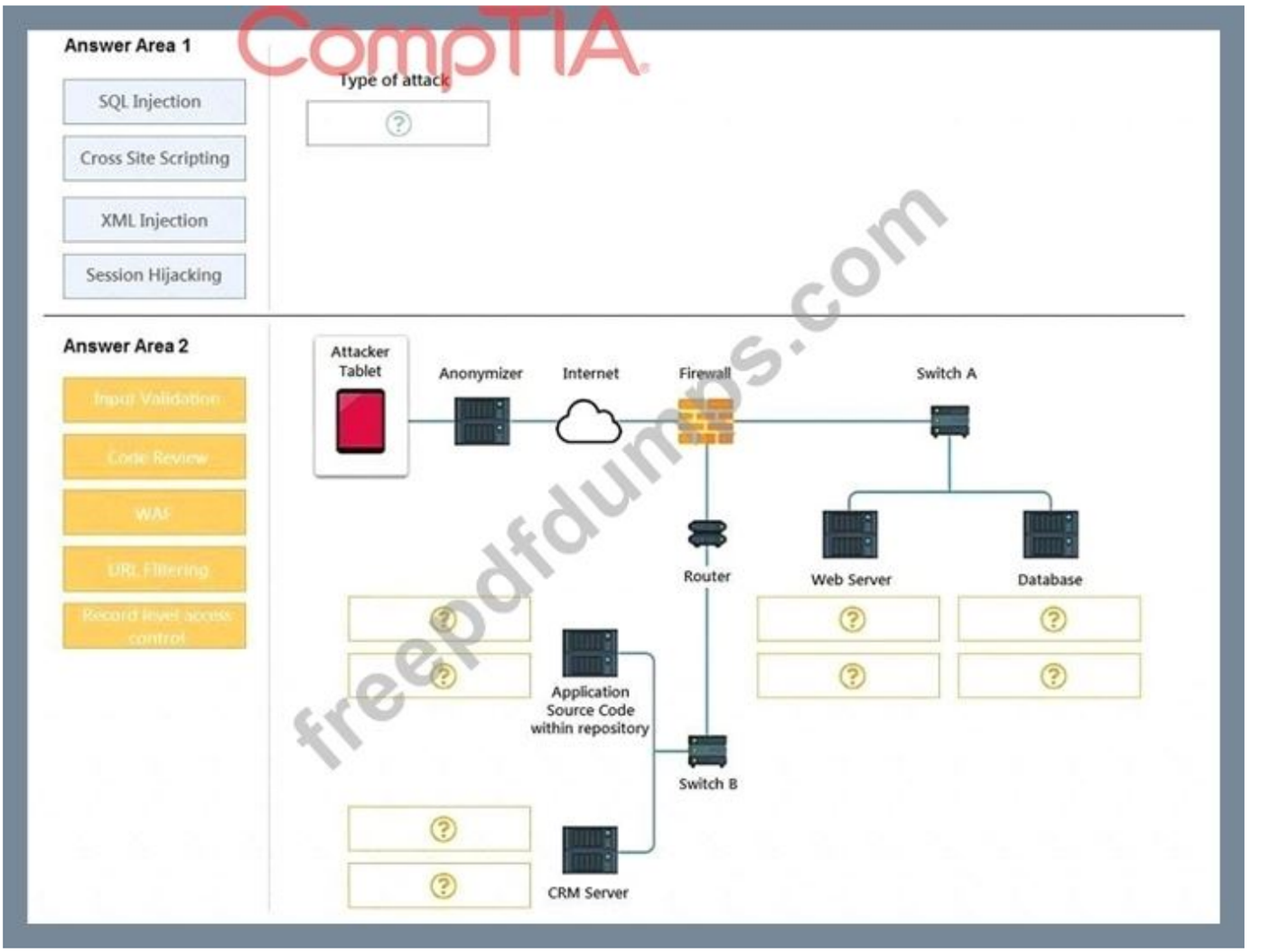
found during the assessment123 References: CompTIA Security+ SY0-601 Certification Study Guide, Chapter 10: Summarizing Risk Management Concepts, page 454; What is a Security Benchmark? - Definition from Techopedia; Security Baselines and Benchmarks - SANS Institute; Security Configuration Benchmarks - CIS

NEW QUESTION: 8
A ecurily analyst b concemed alout iratic initiated to he dark web fom the corporate LAN. Which of the folowing motworks should he analyst monior?
A. SFTP
B. AS
C. Tor
D. LoC
Answer: C (LEAVE A REPLY)

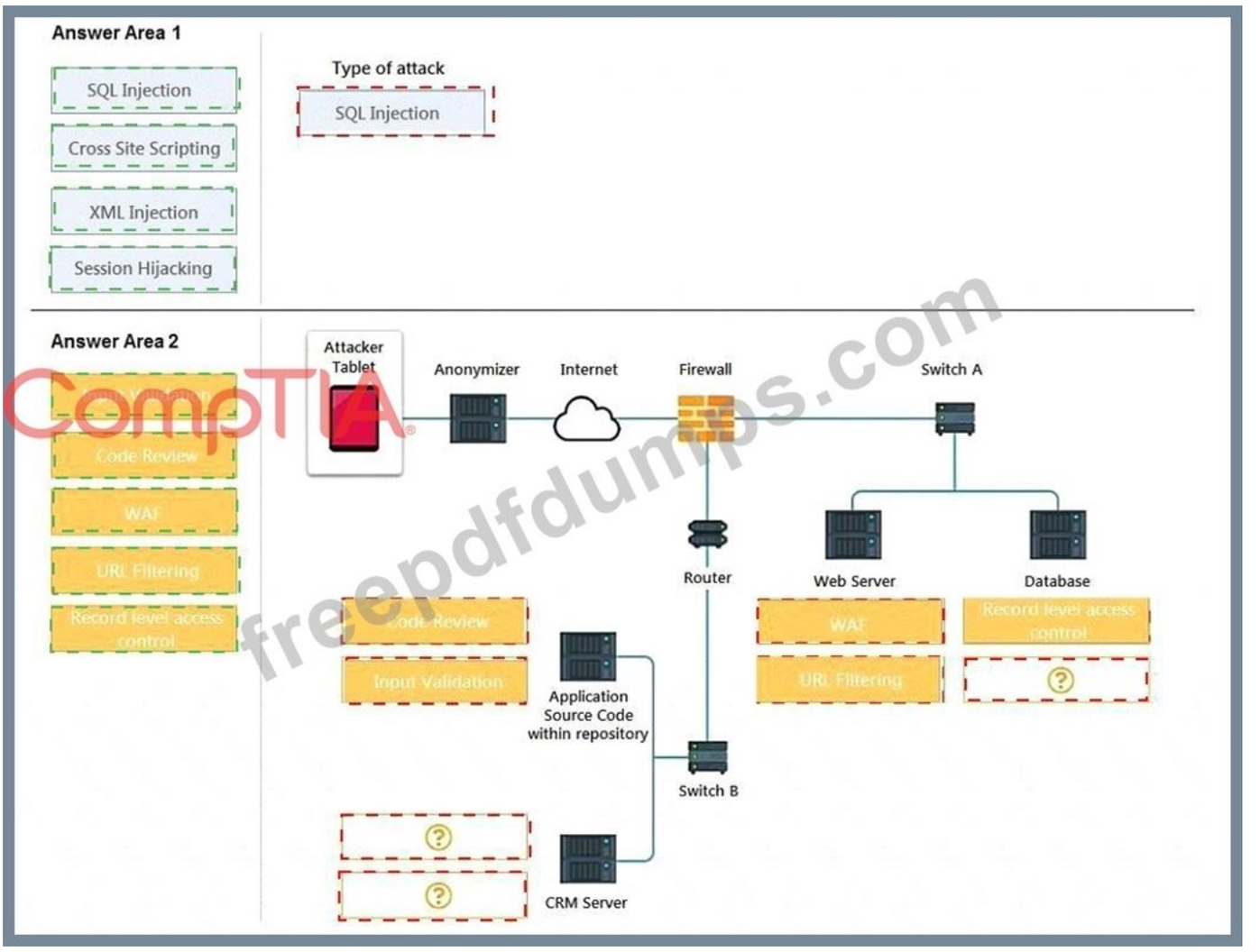
NEW QUESTION: 9
A recent penetration test identified that an attacker could flood the MAC address table of network switches.
Which of the following would best mitigate this type of attack?
A. IPS
B. Load balancer
C. NGFW
D. Port security
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
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.

Select and Place:

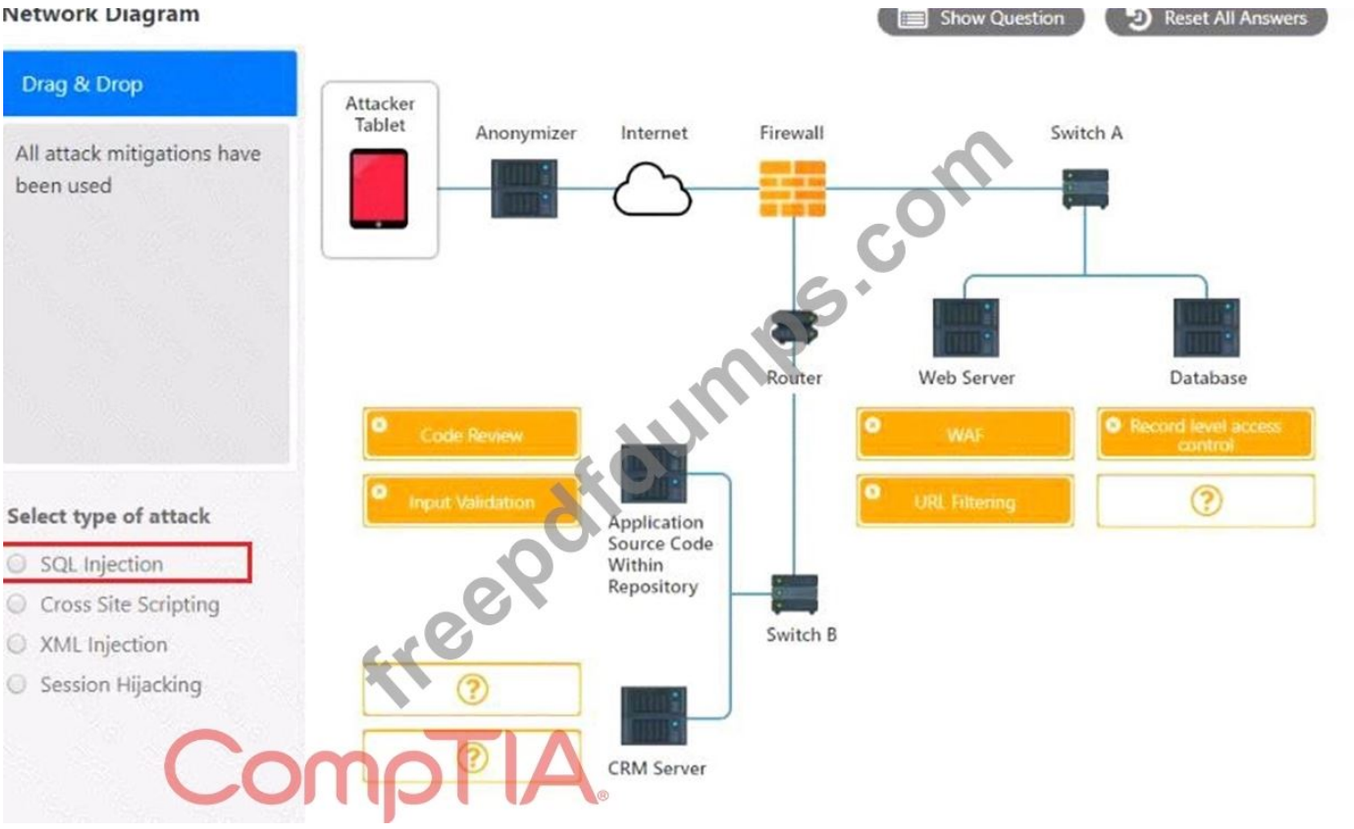

Answer Area 1
Type of attack
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Answer Area 2
Input Validation
Code Review
WAF
URL Filtering
Record level access control
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Application Source Code within repository
Switch B
CRM Server

Answer:



Explanation

A computer screen shot of a computer Description automatically generated with low confidence



NEW QUESTION: 11
Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?
A. Order of volatility
B. Preservation of event logs
C. Chain of custody
D. Compliance with legal hold
Answer: A (LEAVE A REPLY)
The order of volatility is a concept in digital forensics and incident response that refers to the sequence in which different types of data should be preserved or collected during an investigation, based on their likelihood to change or be lost. The general principle is to start with the most volatile data first, as it is more prone to alteration or loss, and then proceed to less volatile data. The order of volatility typically follows a hierarchy from more volatile to less volatile data.

NEW QUESTION: 12
While checking logs, a security engineer notices a number of end users suddenly downloading files with the
.tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment.
Answer: (SHOW ANSWER)
Explanation
https://www.howtogeek.com/362203/what-is-a-tar.gz-file-and-how-do-i-open-it/

NEW QUESTION: 13
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:
A. whaling.
B. smishing.
C. spear phishing
D. vishing
Answer: C (LEAVE A REPLY)
The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. Reference: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

NEW QUESTION: 14
A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

Answer:

NEW QUESTION: 15
A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?
A. S/MIME
B. LDAPS
C. SSH
D. SRTP
Answer: C (LEAVE A REPLY)
SSH - SSH or (Secure Shell) is a protocol that enables two computers to communicate securely by encrypting the connection. Since the question is looking to transfer files over the internet to a specific directory, the FTP protocol can be used for the file transfer itself. As SSH can be used with the FTP protocol, this allows for secure(SSH) file transfer(FTP) over the internet.
S/MIME (Secure/Multipurpose internet Mail Extensions) - Digitally signs and encrypts the contents of email messages.
LDAPS(Lightweight Directory Access Protocol) - Provides authentication for directory-based traffic.
SRTP (Secure Real-time Transport Protocol) - Provides authentication/encryption for transmitted audio and video traffic.

NEW QUESTION: 16
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box.

Which of the following should be the first lines of defense against such an attack? (Choose two.)
A. MAC filtering
B. Zero Trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards
Answer: D,E (LEAVE A REPLY)
We are asked for the first line of defense. Not the most versatile, or best combination. What if we had it all, which ones would be the first two. Well we have to stop the adversaries from entering the facility of course. Access control vestibules and guards do this. Then we have the more technical solutions such as Mac filtering or NAC, but as I noted, we need to pick the two which would be our first line of defense.

NEW QUESTION: 17
Data exftitration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server Which of the following attacks explains what occurred? (Select TWO)
A. Privilege escalation
B. SQL injection
C. Pass-the- hash
D. Directory traversal
E. Request forgery
F. Cross-site scnpting
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?
A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.

C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.
Answer: D (LEAVE A REPLY)
An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. Reference: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION: 19
A security engineer is reviewing log files after a third party discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one week earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?
A. Man-in-the middle
B. Spear-phishing
C. Evil twin
D. DNS poising
Answer: D (LEAVE A REPLY)
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).
https://en.wikipedia.org/wiki/DNS_spoofing

NEW QUESTION: 20
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?
A. Time stamp
B. Chain of custody
C. Admissibility
D. Legal hold
Answer: (SHOW ANSWER)
Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.

NEW QUESTION: 21
Which of the following is most likely to include a SCADA system?
A. Wi-Fi-enabled thermostat
B. Water treatment plant
C. Smart watch
D. Surveillance system
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
Earlier in the week, the CSIRT was alerted to a cyber-incident. The CSIRT is now interacting with the affected systems in an attempt to stop further damage. Which of the following best describes this phase of the incident response process?
A. Preparation
B. Recovery
C. Eradication
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 23
A global pandemic is forcing a private organization to close some business units and reduce staffing at others.
Which of the following would be BEST to help the organization's executives determine the next course of action?
A. A business continuity plan
B. A communications plan
C. An incident response plan
D. A disaster recovery plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?
A. The signal on the WAP needs to be increased in that section of the building.
B. The certificates have expired on the devices and need to be reinstalled.
C. An external access point is engaging in an evil-twin attack.
D. The users in that section of the building are on a VLAN that is being blocked by the firewall.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
A company is under investigation for possible fraud. As part of the investigation the authorities need to renew all emails and ensure data is not deleted. Which of the following company implement to assist in the investigation?
A. Content filter
B. Chain of custody
C. Data loss prevention
D. Legal hold
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?
A. SIEM
B. CASB
C. UTM
D. DLP
Answer: B (LEAVE A REPLY)
Microsoft has a straightforward definition and it includes DLP. "is a security policy enforcement point positioned between enterprise users and cloud service providers" https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb A cloud access security broker (CASB) works by securing data flowing to and from in-house IT architectures and cloud vendor environments using an organization's security policies. CASBs protect enterprise systems against cyberattacks through malware prevention and provide data security through encryption, making data streams unreadable to outside parties. CASBs were created with one thing in mind: protecting proprietary data stored in external, third-party media. CASBs deliver capabilities not generally available in traditional controls such as secure web gateways (SWGs) and enterprise firewalls. CASBs provide policy and governance concurrently across multiple cloud services and provide granular visibility into and control over user activities. https://www.forcepoint.com/cyber-edu/casb-cloud-access-security-broker

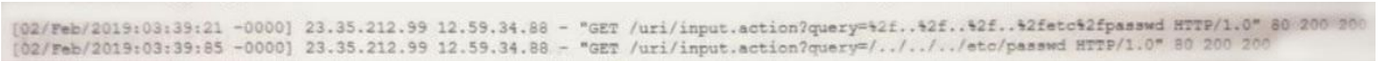
NEW QUESTION: 27
Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?
A. EF x asset value
B. ALE / SLE
C. MTBF x impact
D. SLE x ARO
Answer: (SHOW ANSWER)

Explanation
The total loss expected per year due to a threat targeting an asset can be calculated using the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE is the monetary loss expected from a single event, while ARO is the estimated frequency of that event occurring in a year.
Reference: CompTIA Security+ Study Guide: Exam SY0-501, 7th Edition, by Emmett Dulaney and Chuck Easttom, Chapter 9: Risk Management, page 414.

NEW QUESTION: 28
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 reduce the resilience and availability of system if the provider goes offline.
B. SSO would reduce the password complexity for frontline staff.
C. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
D. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
Answer: (SHOW ANSWER)

NEW QUESTION: 29
A user is concerned that a web application will not be able to handle unexpected or random input without crashing.
Which of the following BEST describes the type of testing the user should perform?
A. Manual code review
B. Fuzzing
C. Dynamic code analysis
D. Code signing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
A security analyst sees the following log output while reviewing web logs:



Which of the following mitigation strategies would be BEST to prevent this attack from being successful?
A. Code signing
B. Stored procedures
C. Input validation
D. Secure cookies

Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.
Which of the following best describes this step?
A. Capacity planning
B. Redundancy
C. Geographic dispersion
D. Tabletop exercise
Answer: A (LEAVE A REPLY)
Explanation
Capacity planning is the process of determining the resources needed to meet the demand for a service or product. It involves estimating the number of staff members required to sustain the business in the case of a disruption, as well as other factors such as equipment, space, and budget Redundancy, geographic dispersion, and tabletop exercise are not directly related to determining the staff members needed for business continuity. Redundancy is the duplication of critical components or functions to increase reliability and availability . Geographic dispersion is the distribution of resources across different locations to reduce the impact of a localized disaster . Tabletop exercise is a simulation of a potential scenario that tests the effectiveness of a business continuity plan

NEW QUESTION: 32
A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?
A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls
Answer: C (LEAVE A REPLY)
Explanation

Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.
In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:
* Encrypting data on removable media
* Scanning removable media for malware before use
* Restricting access to removable media ports
* Implementing policies and procedures for removable media usage and disposal
* Educating users on the risks and best practices of removable media

NEW QUESTION: 33
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?
A. Quarantining
B. Tuning
C. Aggregating
D. Archiving
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?
A. Public
B. Community
C. Hybrid
D. Private
Answer: (SHOW ANSWER)
Hybrid cloud since internal network and cloud computing is combined.
Private cloud = A cloud infrastructure setup and intended specifically for one client/customer.
Community Cloud = A cloud infrastructure shared by organizations within the same industry. "Communitizes" the costs of cloud computing to reduce the cost burden per entity. Such as banking organizations going in together on a community cloud platform designed specifically for the banking industries cloud computing needs.

Hybrid = A mixed model where computing, storage, and applications are both on-premise and in the cloud, as well as utilizing more than one cloud service. Most organizations are a hybrid cloud.
Public = Any cloud service offered to the general public. Ranging from Google Drive, Microsoft Azure, Amazon Web Services, and Microsoft OneNote.

NEW QUESTION: 35
Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?
A. Compensating
B. Deterrent
C. Preventive
D. Detective
Answer: C (LEAVE A REPLY)
The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware.
According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

NEW QUESTION: 36
Which of the following organizations sets frameworks and controls for optimal security configuration on systems?
A. GDPR
B. NIST
C. ISO
D. PCI DSS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
Joe. a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

Which of the following can be determined about the organization's public presence and security posture?
(Select TWO).

A. The organization has adequate information available in public registration.

B. The organization has too much information available in public registration.

C. Joe used cURL to produce this output.

D. Joe used Who is to produce this output.

E. The organization has too little information available in public registration

F. Joe used Wireshark to produce this output

Answer: (SHOW ANSWER)

NEW QUESTION: 38

A company has been experiencing very brief power outages from its utility company over the last few months.
These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

A. Dual power supplies

B. A UPS

C. APDU

D. A generator

Answer: B (LEAVE A REPLY)

NEW QUESTION: 39

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Digital signature

B. Hashing
C. Integrity
D. Salting
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following components can be used to consolidate and forward inbound Interne! traffic to multiple cloud environments though a single firewall?
A. Transit gateway
B. Edge computing
C. Cloud hot site
D. DNS sinkhole
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analyst are spending a long time to trace information on different cloud consoles and correlating data in different formats.
Which of the following can be used to optimize the incident response time?
A. VPC
B. CASB
C. SWG
D. CMS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
A security analyst it investigating an incident to determine what an attacker was able to do on a compromised Laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

A. An attacker was able to move laterally from PC 1 to PC2 using a pass-the-hash attach

B. An attacker was able to bypass the application approve list by emailing a spreadsheet. attachment with an embedded PowerShell in the file.

C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook

D. An attacker was able to phish user credentials successfully from an Outlook user profile

Answer: B (LEAVE A REPLY)

Explanation

The SIEM log shows that the user opened an email attachment named "Invoice.xlsx" and then executed a PowerShell script that downloaded and ran a malicious file from a remote server. This indicates that the attacker was able to bypass the application approve list by emailing a spreadsheet attachment with an embedded PowerShell in the file. This is a common technique used by malware authors to evade detection and deliver their payloads1.

NEW QUESTION: 43

Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the Internet. No business emails were identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounts. Which of the following would mitigate the issue?

A. Complexity requirements

B. Password history
C. Acceptable use policy
D. Shared accounts
Answer: B (LEAVE A REPLY)
Password history policies determines the number of unique new passwords that must associated with a user's account before an old password be reused. Essentially forcing users to create new passwords on a regular basis.
For this situation, forcing users to use new unique passwords would somewhat mitigate the issue.

NEW QUESTION: 44
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?
A. GDPR
B. PCI DSS
C. ISO 27000
D. NIST 800-53
Answer: D (LEAVE A REPLY)
NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION: 45
Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?
A. The business continuity plan
B. The retention policy
C. The disaster recovery plan
D. The incident response plan
Answer: A (LEAVE A REPLY)
Explanation
BCP is to empower an organization to keep crucial functions running during downtime. This, in turn, helps the organization respond quickly to an interruption, while creating resilient operational protocols.

NEW QUESTION: 46
A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?
A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports
C. A zero-day vulnerability was used to exploit the web server
D. The scan reported a false negative for the vulnerability
Answer: A (LEAVE A REPLY)
Explanation
A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers.
Security patches are essential for maintaining the security and functionality of systems and applications.
If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.
The other options are not correct because:
* B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.
* C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.
* D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.
According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:
"A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers." References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/

NEW QUESTION: 47
As accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?
A. Implementing insider threat detection measures
B. Standardizing security incident reporting
C. Executing regular phishing campaigns
D. Updating processes for sending wire transfers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?
A. Smishing
B. Phishing
C. Impersonating
D. Vishing
Answer: (SHOW ANSWER)
The attacker in this scenario is using "Vishing" (Option D). Vishing stands for "voice phishing," and it involves a social engineering attack where an attacker makes phone calls, impersonates someone they are not, and tries to manipulate the victim into revealing sensitive information or taking specific actions, such as purchasing gift cards. In this case, the attacker is posing as the CEO and attempting to trick the employee over the phone.

NEW QUESTION: 49
Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).
Testing security systems and processes regularly
A. Assigning a unique ID to each person with computer access
B. Encrypting transmission of cardholder data across private networks
C. Benchmarking security awareness training for contractors
D. Installing and maintaining a web proxy to protect cardholder data
E. Using vendor-supplied default passwords for system passwords
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Internet of Things
B. Infrastructure as code
C. Software-defined networking
D. Software as a service
Answer: (SHOW ANSWER)

NEW QUESTION: 51
An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?
A. TLS
B. SD-WAN
C. NGFW
D. WAF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
An amusement park is implementing a btomelnc system that validates customers' fingerpnnts to ensure they are not sharing tickets The park's owner values customers above all and would prefer customers' convenience over security For this reason which of the following features should the security team prioritize FIRST?
A. Low FAR
B. Low efficacy
C. Low FRR
D. Low CER
Answer: (SHOW ANSWER)
FAR (False Acceptance Rate)
FRR (False Rejection Rate)
CER (Crossover Error Rate) AKA ERR (Equal Error Rate)
since he is willing to sacrifice Security for Customer Service, Best way to understand this is.
FAR has to go up in order for FRR to go down.
typical business practice is in the middle of both which would be near the CER.

NEW QUESTION: 53
A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?
A. Bluejacking
B. Jamming
C. Rogue access point
D. Evil twin

Answer: D (LEAVE A REPLY)
An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION: 54
he SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network.
An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?
A. The vulnerability management team
B. The NOC team
C. The CIRT
D, The red team
Answer: (SHOW ANSWER)

NEW QUESTION: 55
The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?
A. Acceptable use
B. Clean desk
C. Access control
D. Password complexity
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload. Which of the following attacks did the analyst observe?
A. Privilege escalation
B. Request forgeries
C. Injection
D. Replay attack
Answer: (SHOW ANSWER)

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.[2] There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.[3] In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

NEW QUESTION: 57
A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?
A. Logic Bomb
B. Ransomware
C. Fileless virus
D. Remote access Trojans
E. Rootkit
Answer: (SHOW ANSWER)
"software was configured to delete data deliberately from those servers" This could be achieved by a cronjob.

NEW QUESTION: 58
A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. Which of the following concepts should the administrator utilize?
A. Provisioning
B. Staging
C. Development
D. Quality assurance
Answer: A (LEAVE A REPLY)
Provisioning is the process of creating and setting up IT infrastructure, and includes the steps required to manage user and system access to various resources . Provisioning can be done for servers, cloud environments, users, networks, services, and more .
In this case, the security administrator wants to ensure that all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. This means that the

administrator needs to provision the cloud servers with the necessary software and configuration before they are deployed or used by customers or end users. Provisioning can help automate and standardize the process of setting up cloud servers and reduce the risk of human errors or inconsistencies.

NEW QUESTION: 59
An employee finds a USB flash drive labeled "Salary Info" in an office parking lot. The employee picks up the USB flash drive, goes into the office, and plugs it into a laptop. Later, a technician inspects the laptop and realizes it has been compromised by malware. Which of the following types of social engineering attacks has occurred?
A. Smishing
B. Pretexting
C. Tailgating
D. Baiting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
A company has installed badge readers for building access but is finding unauthorized individuals roaming the hallways. Which of the following is the most likely cause?
A. Shoulder surfing
B. Identity fraud
C. Phishing
D. Tailgating
Answer: (SHOW ANSWER)

NEW QUESTION: 61
A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng. the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?
A. On-path
B. Jamming
C. Rogue access point
D. Evil twin
E. Disassociation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 62
An analyst has determined that a server was not patched and an external actor exfiltrated 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 correlation of events
B. The baseline report
C. The vulnerability scan output
D. The security logs
Answer: (SHOW ANSWER)

NEW QUESTION: 63
A company is looking to move completely to a remote work environment. The Chief Information Security Officer is concerned about the improper use of company-owned devices when employees are working from home. Which of the following could be implemented to ensure that devices are on the company-owned network?
A. Internet proxy
B. Always-on VPN
C. Split tunneling
D. OS firewall
Answer: B (LEAVE A REPLY)
Explanation
Always-on VPN is a feature that enables the active VPN profile to connect automatically on certain triggers, such as user sign-in, network change, or device screen on. This ensures that the devices are always on the company-owned network and protected by the company's security policies. Always-on VPN also prevents the devices from accessing the internet if the VPN connection is lost or interrupted

NEW QUESTION: 64
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 (LEAVE A REPLY)
Explanation
ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware, p. 7

NEW QUESTION: 65
A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?
A. DLP
B. SIEM
C. NIDS
D. WAF
Answer: (SHOW ANSWER)
WAF stands for Web Application Firewall, which is a type of firewall that can monitor, filter and block web traffic to and from web applications. WAF can protect web applications from common attacks such as cross-site scripting (XSS), SQL injection, directory traversal, buffer overflow and more. WAF can also enforce security policies and rules that can prevent parameter manipulation or tampering by an unknown third party. WAF is the best solution to help protect against the attack on the web API, as it can inspect the HTTP requests and responses and block any malicious or anomalous activity. Verified Reference:
Other Application Attacks - SY0-601 CompTIA Security+ : 1.3
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/other-application-attacks/ (See Web Application Firewall) CompTIA Security+ SY0-601 Exam Cram
https://www.oreilly.com/library/view/comptia-security-sy0-601/9780136798767/ch03.xhtml (See Web Application Firewall) Security+ domain #1: Attacks, threats, and vulnerabilities [updated 2021] https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/ (See Web application firewall)

NEW QUESTION: 66
Historically, a company has had issues with users plugging in personally owned removable media devices into corporate computers. As a result, the threat of malware incidents is almost constant.

Which of the following would BEST help prevent the malware from being installed on the computers?

A. NGFW

B. EDR

C. AUP

D. DLP

Answer: (SHOW ANSWER)

NEW QUESTION: 67

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.

B. The workstations are beaconing to a command-and-control server.

C. A logic bomb was executed and is responsible for the data transfers.

D. A fireless virus is spreading in the local network environment.

Answer: A (LEAVE A REPLY)

RATs are typically downloaded together with a seemingly legitimate program, like a game, or are sent to the target as an email attachment. Once the attacker compromises the host's system, they can use it to distribute RATs to additional vulnerable computers, establishing a botnet.

NEW QUESTION: 68

Which of the following algorithms has the SMALLEST key size?

A. RSA

B. DES

C. Twofish

D. AES

Answer: (SHOW ANSWER)

NEW QUESTION: 69

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: A (LEAVE A REPLY)

Explanation

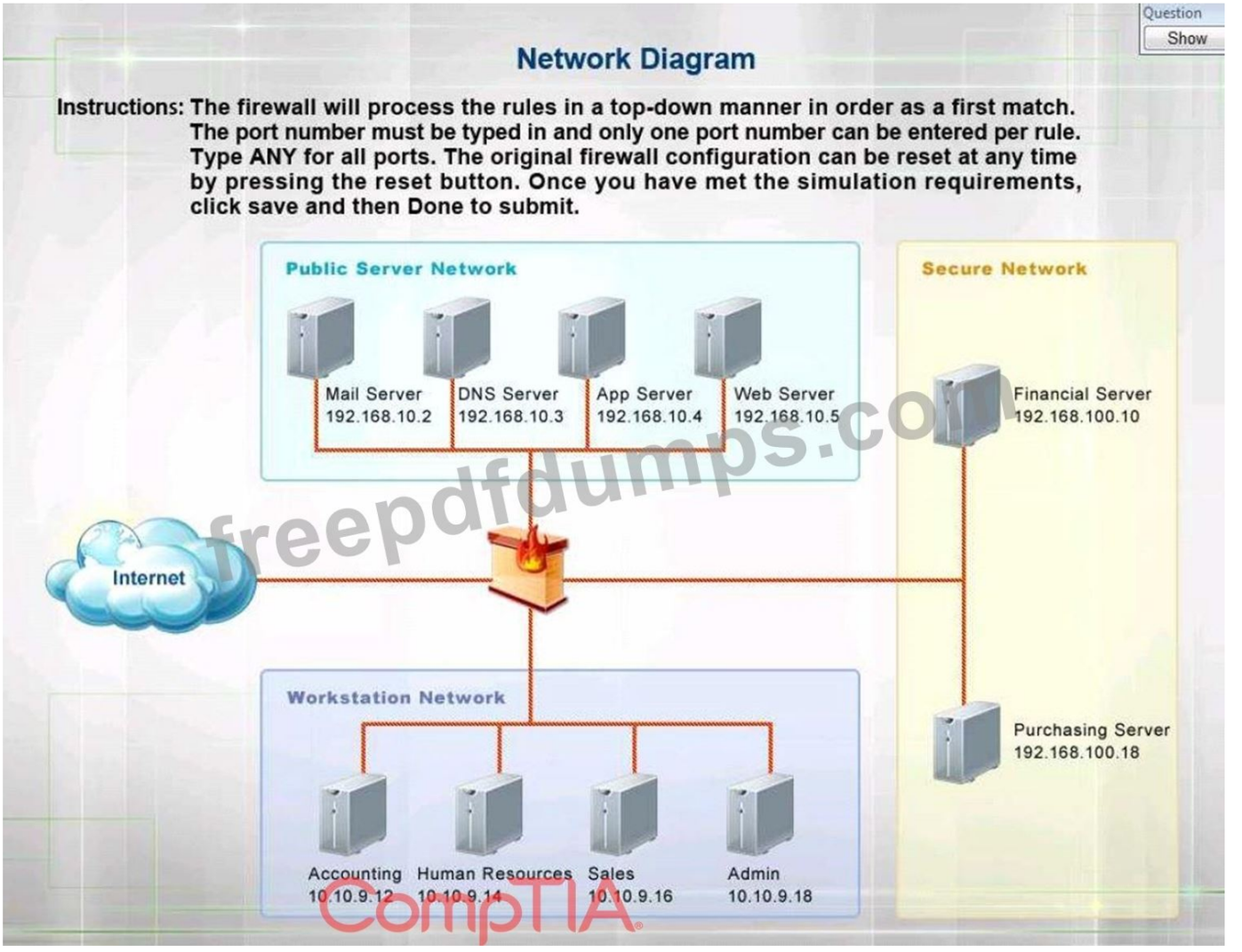
https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/

NEW QUESTION: 70
During a security incident the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9 A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?
A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32
Answer: B (LEAVE A REPLY)
Explanation
This command creates an inbound access list that denies any IP traffic from the source IP address of
10.1.4.9/32 to any destination IP address (0.0.0.0/0). It blocks the originating source of malicious traffic from accessing the organization's network.

NEW QUESTION: 71
A security researcher has alerted an organization that its sensitive user data was found for sale on a website.
Which of the following should the organization use to inform the affected parties?
A. An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan
Answer: (SHOW ANSWER)
A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION: 72
The security administrator has installed a new firewall which implements an implicit DENY policy by default.
Answer:
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

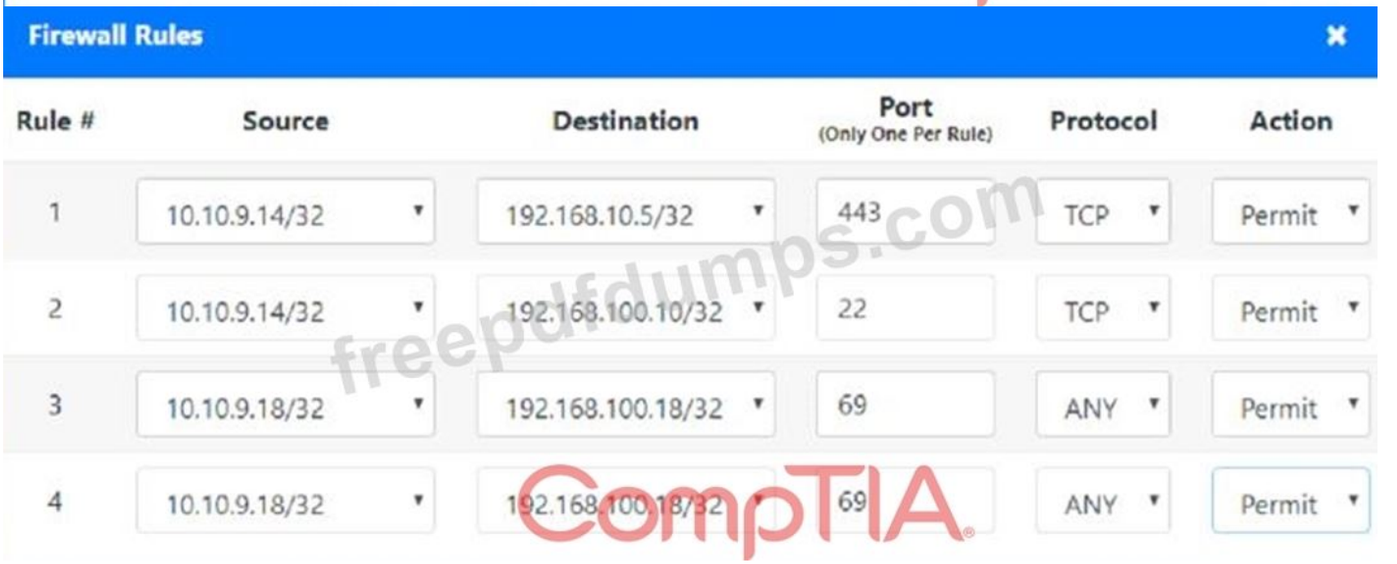
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.
Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type 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.



Hot Area:

Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny



Section: Network Security

Explanation:

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 22 Rule #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 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

NEW QUESTION: 73

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII

B. TLP

C. TTP

D. STIX

Answer: C (LEAVE A REPLY)

Explanation

TTPs Within Cyber Threat Intelligence

* Tactics, techniques and procedures (TTPs) are the "patterns of activities or methods associated with a specific threat actor or group of threat actors."

* Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks.

* Top threats facing an organization should be given priority for TTP maturation. Smaller organizations may benefit strategically by outsourcing research and response.

One acronym everyone working on a cybersecurity team should be familiar with is TTPs - tactics, techniques and procedures - but not everyone understands how to use them properly within a cyber threat intelligence solution. TTPs describe how threat actors (the bad guys) orchestrate, execute and manage their operations attacks. ("Tactics" is also sometimes called "tools" in the acronym.) Specifically, TTPs are defined as the

"patterns of activities or methods associated with a specific threat actor or group of threat actors," according to the Definitive Guide to Cyber Threat Intelligence.

NEW QUESTION: 74

Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

A. Vulnerability scanner

B. Open-source intelligence

C. Packet capture

D. Threat feeds

Answer: (SHOW ANSWER)

Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds, analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.

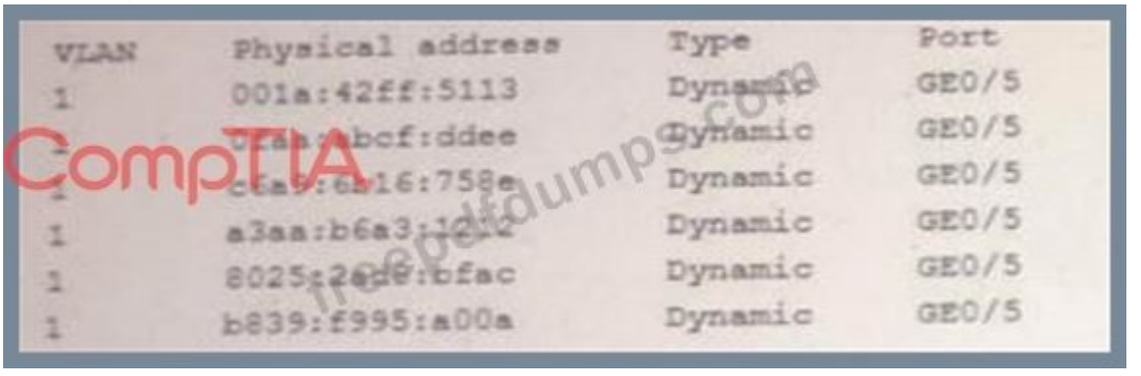
References:

1. CompTIA Security+ Certification Exam Objectives (SY0-601):

https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf
2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively:
https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367

NEW QUESTION: 75
A security monitoring company offers a service that alerts its customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?
A. STIX
B. The dark web
C. Social media
D. TAXI
E. PCI
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
A security administrator checks the table of a network switch, which shows the following output:



Which of the following is happening to this switch?
A. ARP poisoning
B. MAC cloning
C. DNS poisoning
D. MAC Flooding
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

A. SED

B. HSM

C. DLP

D. TPM

Answer: (SHOW ANSWER)

Explanation

SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine1. SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

NEW QUESTION: 78

An organization wants to ensure the integrity of compiled binaries in the production environment. Which of the following security measures would best support this objective?

A. Input validation

B. Code signing

C. Static analysis

D. SQL injection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?

A. CASB

B. VPN concentrator

C. MFA

D. VPC endpoint

Answer: (SHOW ANSWER)

Explanation

A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. References:

CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

NEW QUESTION: 80

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL

B. Implement a network-wide scan for other instances of the malware.

C. Quarantine the host from other parts of the network

D. Revoke the client's network access certificates

Answer: B (LEAVE A REPLY)

What is Malware?

Malware, short for "malicious software," refers to any intrusive software developed by cybercriminals (often called "hackers") to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

How do I detect and respond to malware?

Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats. Learn how to update your antivirus strategy.

NEW QUESTION: 81

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

A. Alarms

B. Signage

C. Lighting

D. Access control vestibules

E. Fencing

F. Sensors

Answer: D,E (LEAVE A REPLY)

Explanation

Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical countermeasure and Sensors are either reactive or technical.

https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/

NEW QUESTION: 82
A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols.
A security engineer runs a port scan against the server from the Internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?
A. Block HTTPS access from the Internet
B. Block SMTP access from the Internet
C. Block SSH access from the Internet.
D. Allow DNS access from the internet.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
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. RADIUS
B. Active Directory
C. DNSSEC
D. Reverse proxy
E. VPN concentrator
F. PKI
Answer: A,F (LEAVE A REPLY)

NEW QUESTION: 84
A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away. Which of the following solutions should the CISO implement?
A. VAF
B. SWG
C. VPN
D. WDS
Answer: B (LEAVE A REPLY)

A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service. References: https://www.comptia.org/content/guides/what-is-a-secure-web-gateway

NEW QUESTION: 85
When implementing automation with IoT devices, which of the following should be considered first to keep the network secure?
A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols
Answer: D (LEAVE A REPLY)
Communication protocols are the rules and standards that govern how devices communicate over a network.
They are essential for ensuring security, reliability, and compatibility among different IoT devices. Some examples of communication protocols for IoT are MQTT, CoAP, HTTP, and Zigbee.

NEW QUESTION: 86
Which of the following is the correct order of volatility from most to least volatile?
A. Memory, temporary filesystems. routing tables, disk, network storage
B. Cache, memory, temporary filesystems. disk, archival media
C. Memory, disk, temporary filesystems. cache, archival media
D. Cache, disk, temporary filesystems. network storage, archival media
Answer: B (LEAVE A REPLY)
The order of volatility is the order of how quickly data can be lost or changed in a system. The order of volatility is important for digital forensics and evidence collection, as it determines the priority and sequence of data preservation. The correct order of volatility from most to least volatile is cache, memory, temporary filesystems, disk, archival media. Cache is the fastest and most volatile type of memory that stores frequently used data. Memory is the main memory or RAM that stores data for active processes. Temporary filesystems are files that are created and deleted during normal system operations, such as swap files, print spool files, etc. Disk is the permanent storage device that stores data on magnetic or solid-state media. Archival media are devices that store data for long-term preservation, such as optical disks, tapes, etc.

NEW QUESTION: 87
A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months.
The organization realizes the need to reassess its security strategy for mitigating risks within the perimeter.

Which of the following solutions would BEST support the organization's strategy?

A. UTM

B. DLP

C. FIM

D. EDR

Answer: A (LEAVE A REPLY)

NEW QUESTION: 88

Which of the following is the most common data loss path for an air-gapped network?

A. Unsecured Bluetooth

B. Unpatched OS

C. Bastion host

D. Removable devices

Answer: D (LEAVE A REPLY)

NEW QUESTION: 89

Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

A. The cameras could be compromised if not patched in a timely manner.

B. An inability to monitor 100%, of every facility could expose the company to unnecessary risk.

C. Exported videos may take up excessive space on the file servers.

D. Physical security at the facility may not protect the cameras from theft.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 90

A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```


Which of the following types of attacks does this MOST likely represent?

A. Rainbow table

B. Brute-force

C. Password-spraying

D. Dictionary

Answer: C (LEAVE A REPLY)
Password spraying is a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

NEW QUESTION: 91
A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?
A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framework
D. ISO 27002
Answer: D (LEAVE A REPLY)
ISO/IEC 27002
ISO/IEC 27002 is an information security standard published by the International Organization for Standardization and by the International Electrotechnical Commission, titled Information technology - Security techniques - Code of practice for information security controls.

NEW QUESTION: 92
Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area?
(Select TWO).
A. Barricades
B. Thermal sensors
C. Drones
D. Signage
E. Motion sensors
F. Guards

G. Bollards

Answer: A,D (LEAVE A REPLY)

Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area. Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 7

NEW QUESTION: 93

Which of the following holds staff accountable while escorting unathorized personal?

A. Locks

B. Cameras

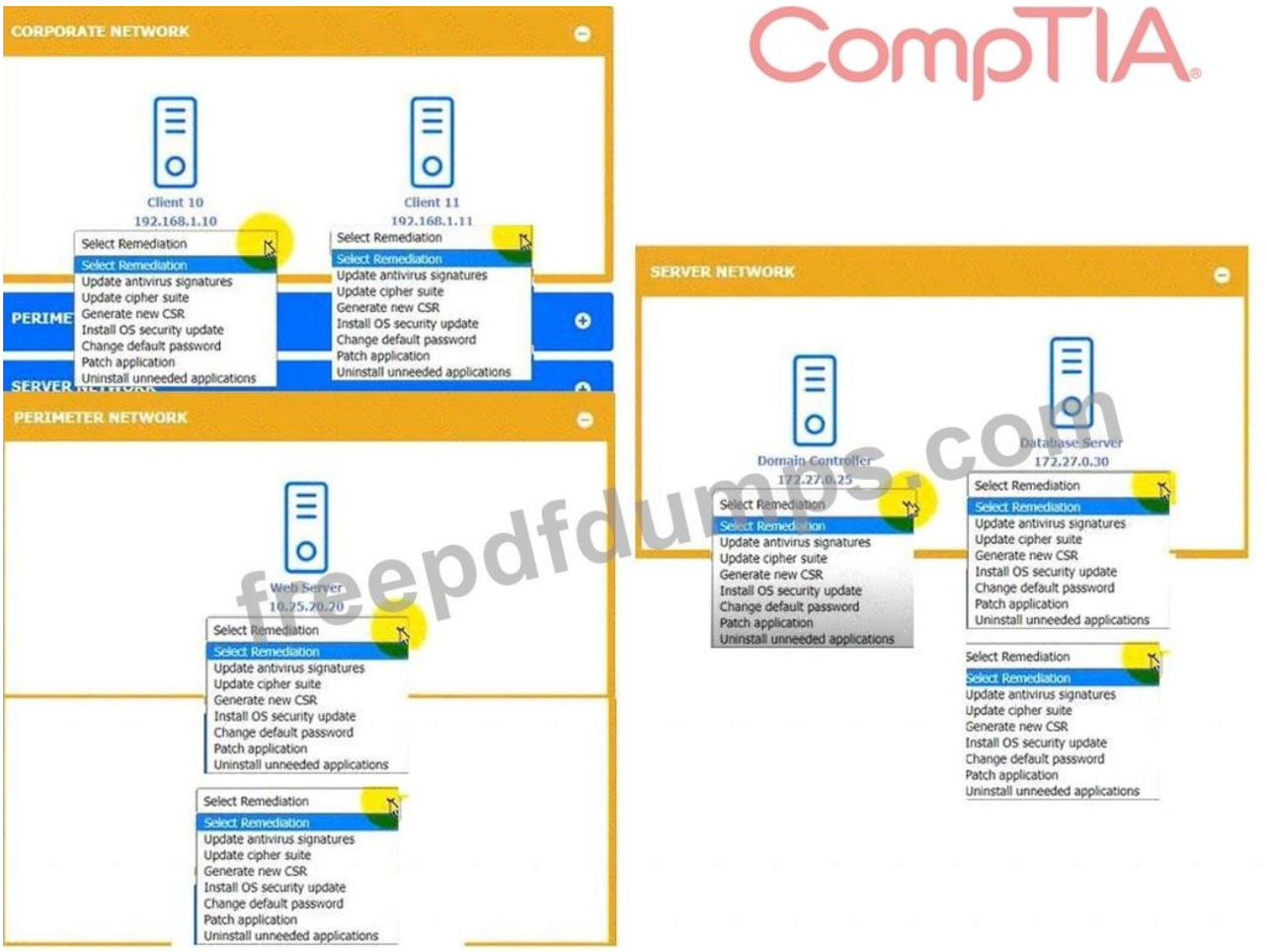
C. Badges

D. Visitor logs

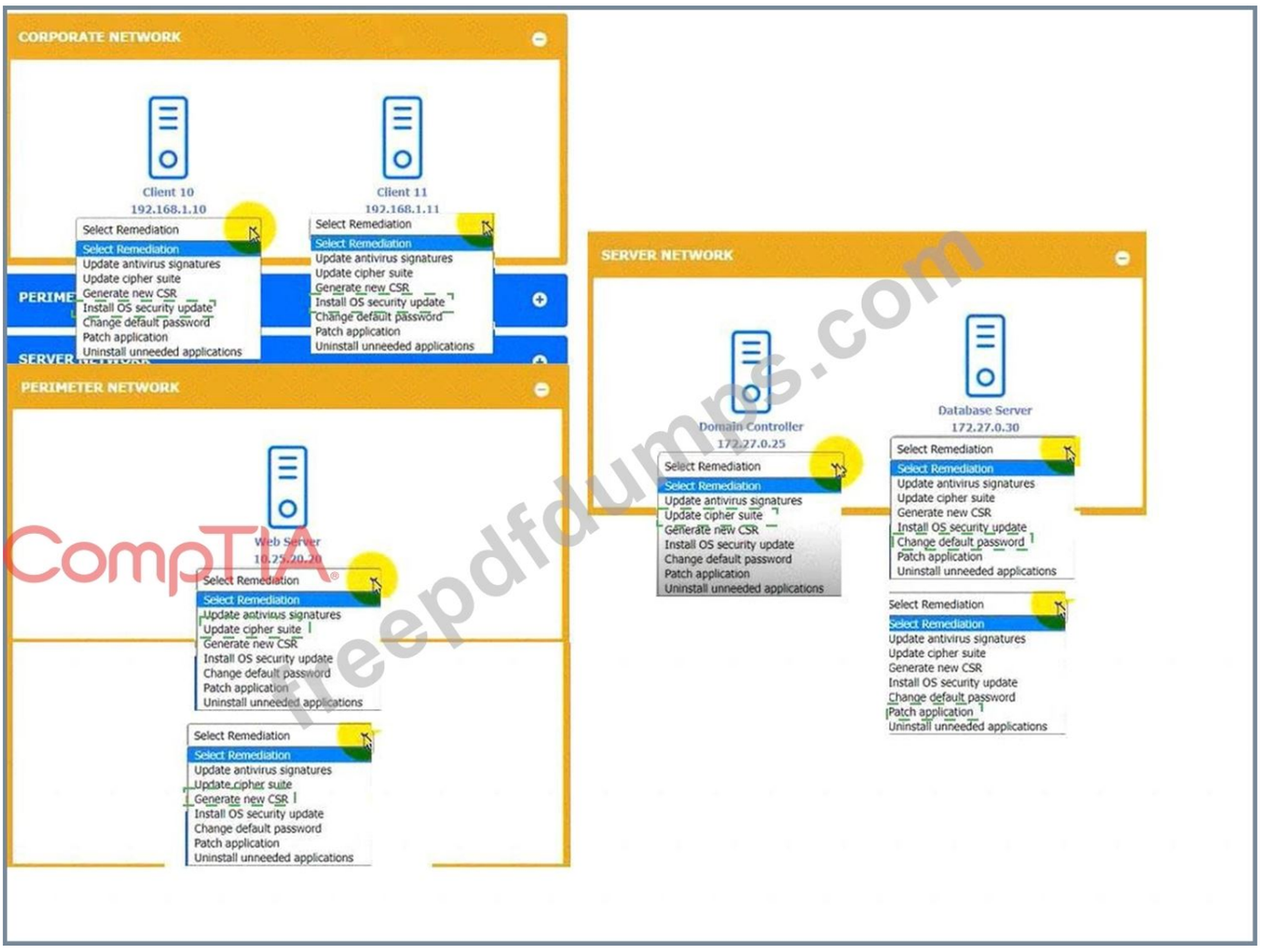
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94

You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or tach dewce.
Remediation options may be selected multiple times, and some devices may require more than one remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.



Answer:



Explanation

Graphical user interface, text, application Description automatically generated

NEW QUESTION: 95

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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Disable vulnerable services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

NEW QUESTION: 96

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications.
Which of the following BEST represents the type of testing that will occur?
A. Gray-box
B. White-box
C. Bug bounty
D. Black-box
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A recent security assessment revealed that an actor explolied a vuinerable workstation willvin an organization and has persisted on the network for several months. The organization realizes the need to reassess Its seourlty strategy for mitigating risks within the perimeter Which of the following solutions woukl BEST support the organization's strategy?
A. FIM
B. OOP
C. EOR
D. DUT
Answer: (SHOW ANSWER)
The best solution to support the organization's security strategy in this situation is File Integrity Monitoring (FIM). FIM is a technique used to detect and monitor unauthorized changes to critical files and system configurations on a computer or network. It is used to detect malicious activity such as malware, unauthorized modifications, and malicious user activity. FIM can also be used to detect and monitor compliance with security policies and procedures.

NEW QUESTION: 98
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. DNS hijacking
C. URL redirection

D. ARP poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue.
Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?
A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alerts.
Answer: (SHOW ANSWER)
Explanation
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION: 100
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	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

NEW QUESTION: 101
A company would like to implement a network security solution to inspect traffic on the network and generate an alert when specific traffic patterns are observed. The solution should never block legitimate network traffic. Which of the following will the company most likely implement?
A. ACLs
B. WAF
C. HIPS
D. NIDS
Answer: (SHOW ANSWER)

NEW QUESTION: 102
A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?
A. Verification
B. Validation
C. Normalization
D. Staging
Answer: B (LEAVE A REPLY)
Verification does not involve code execution while Validation involves code execution. Verification uses methods like reviews, walkthroughs, inspections and desk-checking whereas Validation uses methods like black box testing, white box testing and non-functional testing.

NEW QUESTION: 103
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

GET http://yourbank.com/transfer.do?acctnum=08764 6959 &amount=500000 HTTP/1.1 GET http://yourbank.com/transfer.do?acctnum=087646958 &amount=5000000 HTTP/1.1 GET http://yourbank.com/transfer.do?acctnum=-087646958 &amount=1000000 HTTP/1.1 GET http://yourbank.com/transfer.do?acctnum=087646953&amount=500 HTTP/1.1 Which of the following types of attacks is most likely being conducted?

A. SQLi

B. CSRF

C. Spear phishing

D. API

Answer: B (LEAVE A REPLY)

CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated1. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user's session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.

A . SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution2. The output of the web server log does not show any SQL statements or commands.

B . CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials1. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.

C . Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email or message that contains a malicious link or attachment3. The output of the web server log does not show any email or message content or headers.

D . API. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API is not an attack method, but rather a way of designing and developing software applications.

NEW QUESTION: 104

Which of the following are the MOST likely vectors for the unauthorized 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: (SHOW ANSWER)

Plenty of example for vulnerabilities introduced by insecure third party libraries.

NEW QUESTION: 105

Which of the following ISO standards is certified for privacy?

A. ISO 27701

B. ISO 27002

C. ISO 9001

D. ISO 31000

Answer: A (LEAVE A REPLY)