CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization.
Which of the following should be completed FIRST?

A. A business Impact analysis
B. A system assessment
C. Communication of the risk factors
D. A risk identification process

Answer: A

Explanation:
A business impact analysis (BIA) should be completed first before risk calculation and prioritization. A BIA is a process that identifies and evaluates the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, objectives, and strategies for the organization's assets and resources1. A BIA is a prerequisite for risk calculation and prioritization because it provides the basis for estimating the impact and likelihood of various threats and vulnerabilities on the organization's operations, reputation, and finances2.

NEW QUESTION 2
After running the cat file01.bin | hexdump -c command, a security analyst reviews the following output snippet:
00000000 ff d8 ft e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|
Which of the following digital-forensics techniques is the analyst using?

A. Reviewing the file hash
B. Debugging the binary file
C. Implementing file carving
D. Verifying the file type
E. Utilizing reverse engineering

Answer: D

Explanation:
This is the digital-forensics technique that the analyst is using by running the cat file01.bin | hexdump -c command. This command displays the contents of the binary file in hexadecimal and ASCII format, which can help identify the file type based on its header or signature. In this case, the output snippet shows that the file type is JPEG, as indicated by the ff d8 ff e0 bytes at the beginning and the JFIF string in ASCII.

NEW QUESTION 3
An organization wants to collect IoCs from multiple geographic regions so it can sell the information to its customers. Which of the following should the organization deploy to accomplish this task?

A. A honeypot
B. A bastion host
C. A proxy server
D. A Jumpbox

Answer: A

Explanation:
A honeypot is a decoy system that is designed to attract and trap attackers, by mimicking a real system or network, but containing fake or harmless data. A honeypot can be used to collect IoCs from multiple geographic regions, by deploying it in different locations or networks, and monitoring the activities or attacks that target it. A honeypot can also provide valuable threat intelligence data that can be sold to customers.

NEW QUESTION 4
During an audit, several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer. Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products. Which of the following would be the best way to locate this issue?

A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server.
C. Implement input validation.
D. Run a dynamic code analysis.

Answer: C

Explanation:
Implementing input validation is the best way to locate and prevent the issue of manipulation of the
public-facing web form used by customers to order products. Input validation is a technique that checks and filters any user input that is sent to an application before processing it. Input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the application. Input validation can also reject or sanitize any input that does not meet the validation criteria .

NEW QUESTION 5
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

A. Make a backup of the server and update the JBoss server that is running on it.

B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Answer: C

Explanation:
What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy"
Creating a proper DMZ for outdated components and segregating the JBoss server is the best action to take first to prevent server compromise and business disruption at the same time. A DMZ (demilitarized zone) is a network segment that separates internal networks from external networks, such as the internet, and provides an additional layer of security3. Creating a proper DMZ for outdated components and segregating the JBoss server can isolate and protect the critical server from external attacks that may exploit its vulnerability.

NEW QUESTION 6
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings
B. Rebooting the phone and installing the latest security updates
C. Documenting the respective chain of custody
D. Uninstalling any potentially unwanted programs
E. Performing a memory dump of the mobile device for analysis
F. Unlocking the device by blowing the eFuse

Answer: CE

Explanation:
Documenting the respective chain of custody and performing a memory dump of the mobile device for analysis would help during the forensic analysis of the mobile device. The chain of custody is a record of who handled the evidence, when, where, how, and why. The chain of custody helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1. A memory dump is a process of capturing and storing the contents of the device's memory (RAM) for analysis. A memory dump can help to recover volatile data that may be lost when the device is powered off or rebooted, such as running processes, network connections, encryption keys, or malware traces2.

NEW QUESTION 7
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

A. Implement UEM on an systems and deploy security software.
B. Implement DLP on all workstations and block company data from being sent outside the company
C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
D. Implement centralized monitoring and logging for an company systems.

Answer: C

Explanation:
A CASB, or Cloud Access Security Broker, is a software tool or service that acts as an intermediary between an organization's cloud services and its users. A CASB can provide various security functions, such as visibility, compliance, threat protection, and data security2
A CASB can help protect the company's data stored in the cloud by preventing certain types of data from being downloaded to a workstation, such as sensitive or confidential information. This can reduce the risk of data leakage, theft, or loss if a workstation is compromised or stolen.

NEW QUESTION 8
A security operations manager wants some recommendations for improving security monitoring. The security team currently uses past events to create an IOC list for monitoring.
Which of the following is the best suggestion for improving monitoring capabilities?

A. Update the IPS and IDS with the latest rule sets from the provider.
B. Create an automated script to update the IPS and IDS rule sets.
C. Use an automated subscription to select threat feeds for IDS.
D. Implement an automated malware solution on the IPS.

Answer: C

Explanation:
Threat feeds are sources of information that provide timely and relevant data about current or emerging cyber threats, such as indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), or threat actors. An IDS, or intrusion detection system, is a tool that monitors network traffic and detects malicious or anomalous activities based on predefined or custom rules. Using an automated subscription to select threat feeds for IDS can help to improve security monitoring capabilities by providing the security team with up-to-date and actionable intelligence that can enhance the detection and response to cyberattacks

NEW QUESTION 9
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

A. Validate the binaries' hashes from a trusted source.
B. Use file integrity monitoring to validate the digital signature
C. Run an antivirus against the binaries to check for malware.
D. Only allow binaries on the approve list to execute.

Answer: A

Explanation:
Validating the binaries' hashes from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

NEW QUESTION 10
During the onboarding process for a new vendor, a security analyst obtains a copy of the vendor's latest penetration test summary:

Severity	Finding count
Critical	2
High	5
Medium	3
Low	2
Informational	4

Performed by: Vendor Red Team Last performed: 14 days ago
Which of the following recommendations should the analyst make first?

A. Perform a more recent penetration test.
B. Continue vendor onboarding.
C. Disclose details regarding the findings.
D. Have a neutral third party perform a penetration test.

Answer: C

Explanation:
The analyst should disclose details regarding the findings of the vendor's latest penetration test summary as the first recommendation, as this can help assess the vendor's security posture and identify any potential risks or issues that may affect the organization. The analyst should review the findings and ask for more information about the scope, methodology, and remediation actions of the penetration test, as well as any evidence or artifacts that support the findings.

NEW QUESTION 10
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USEReroot] [TTY=unknown] [CWD=/home/comptia] [CONMAND=/usr/libexec/gsd-backlight-helper --set-
brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

A. The comptia user knows the sudo password.
B. The comptia user executed the sudo su command.
C. The comptia user knows the root password.
D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: B

Explanation:
The /var/log/secure log file is a file that records security-related events on a Linux system, such as authentication attempts or sudo commands. The log file shows that the comptia user executed the sudo su command, which allows the user to switch to the root account and gain superuser privileges. The log file does not show that the comptia user knows the sudo password, knows the root password, or added himself or herself to the /etc/sudoers file. Reference: https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/

NEW QUESTION 15
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```

Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Uninstall the DNS service
B. Perform a vulnerability scan
C. Change the server's IP to a private IP address
D. Disable the Telnet service
E. Block port 80 with the host-based firewall
F. Change the SSH port to a non-standard port

Answer: DF

Explanation:
Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its functionality as a web server. Reference:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

NEW QUESTION 17
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?

A. Stack counting
B. Searching
C. Clustering
D. Grouping

Answer: A

Explanation:
Stack counting is the best threat-hunting method for the analyst to use to observe and assess the number of times a specific activity occurs and aggregate the results. Stack counting is a technique that involves collecting data from multiple sources, such as logs, events, or alerts, and grouping them by a common attribute, such as an IP address, a user name, or a process name. Stack counting can help identify patterns, trends, outliers, or anomalies in the data that may indicate malicious activity or compromise.

NEW QUESTION 18
An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the Wowing is MOST likely happening?

A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20 30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.

Answer: A

Explanation:
The hosts are most likely part of a reflective denial-of-service attack. A reflective denial-of-service attack is a technique that allows attackers to both magnify the amount of malicious traffic they can generate and obscure the sources of the attack traffic. This type of distributed denial-of-service (DDoS) attack overwhelms the target, causing disruption or outage of systems and services. A reflective denial-of-service attack works by spoofing the target's IP address and sending requests to vulnerable servers that will respond to the target. The servers act as reflectors that bounce back the responses to the target, amplifying the attack volume and hiding the attacker's identity1. The output shows that host 10.20.30.40 is sending requests with a spoofed source IP address of 192.168.1.10 to host 203.0.113.15 on port 123, which is used by the Network Time Protocol (NTP). NTP is a common protocol used for reflection/amplification attacks, as it can generate large responses to small requests2.

NEW QUESTION 21
A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal

Answer: D

Explanation:
A directory traversal attack is a type of web application attack that exploits insufficient input validation or filtering to access files or directories that are outside of the web root folder. A directory traversal attack can allow an attacker to read, modify, or execute files on the target server that are not intended to be accessible via web requests. The URL in the alert contains an example of a directory traversal attack, as indicated by the use of "…/" sequences in the query string. These sequences are used to navigate up one level in the directory hierarchy, potentially reaching sensitive files or folders on the server. In this case, the attacker is

trying to access /etc/passwd file, which contains user account information on Linux systems.

NEW QUESTION 23
A security analyst is monitoring a company's network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.
B. Isolate the system and begin a forensic investigation to determine what was compromised.
C. Recommend network segmentation to the management team as a way to secure the various environments.
D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

Answer: A

Explanation:
Reporting this activity as a false positive, as the activity is legitimate, is the best way for the security analyst to respond. A false positive is a condition in which harmless traffic is classified as a potential network attack by a security monitoring tool. Ping requests are a common network diagnostic tool that can be used to test network connectivity issues. The technician who responded to potential network connectivity issues was performing a legitimate task and did not pose any threat to the accounting and human resources servers .

NEW QUESTION 25
While reviewing abnormal user activity, a security analyst notices a user has the following fileshare activities:

Server	Share	Action
Server001	Confidential	Deny
Server001	HumanResources	Deny
Server002	Temporary	Permit
Server002	Installs	Permit
Server003	Payroll	Deny
Server003	W9Docs	Deny

Which of the following should the analyst do first?

A. Initiate the security incident response process for unauthorized access.
B. Shut down the servers while the access is investigated.
C. Remove the user's access for all fileshares.
D. Lock the user account until the access can be explained.

Answer: A

Explanation:
The security incident response process is a set of procedures and guidelines that define how to identify, contain, analyze, and recover from security incidents that compromise the confidentiality, integrity, or availability of an organization’s assets or operations. Initiating the security incident response process for unauthorized access is the first and most appropriate action that the analyst should take, as it would allow the analyst to follow a structured and consistent approach to handle the situation and mitigate the impact of the incident1.

NEW QUESTION 26
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

A. Enforce the existing security standards and controls.
B. Perform a risk analysis and qualify the risk with legal.
C. Perform research and propose a better technology.
D. Enforce the standard permits.

Answer: B

Explanation:
The International Standards Organization, or ISO, develops standards for businesses around the world so that they may operate using a uniform set of best practices. These standards are not enforceable laws, but companies who choose to follow them stand to gain international credibility from their compliance; standards are set as guidance for best practices but are not enforceable laws

NEW QUESTION 31
Which of the following best explains why it is important for companies to implement both privacy and security policies?

A. Private data is insecure by design, so different programs ensure both policies are addressed.
B. Security policies will automatically ensure the data complies with privacy regulations.
C. Privacy policies will satisfy all regulations to secure consumer and sensitive company data.
D. Both policies have some overlap, but the differences can have regulatory consequences.

Answer: D

Explanation:
The correct answer is D. Both policies have some overlap, but the differences can have regulatory consequences. Privacy and security policies are both important

for companies to protect their data and comply with various laws and regulations. However, privacy and security policies are not the same, and they have different goals and requirements.
Privacy policies are nontechnical controls that define how a company collects, uses, shares, and protects personal information from its customers, employees, or partners. Privacy policies are based on the principles of data minimization, consent, transparency, and accountability. Privacy policies aim to respect the rights and preferences of data subjects and comply with different privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)1.
Security policies are technical or nontechnical controls that define how a company protects its data and systems from unauthorized access, modification, or destruction. Security policies are based on the principles of confidentiality, integrity, and availability. Security policies aim to prevent or mitigate the impact of cyberattacks and comply with different security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or the ISO/IEC 27000 series2.
Privacy and security policies have some overlap, as they both involve data protection and compliance. However, they also have some differences, as they address different aspects and risks of data processing. For example, a company may have a strong security policy that encrypts its data, but it may still violate a privacy policy if it collects or shares more data than necessary or without consent. Conversely, a company may have a clear privacy policy that informs its customers about its data practices, but it may still suffer a security breach if it does not implement adequate security measures3.

NEW QUESTION 35
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

A. Warn the incident response team that the server can be compromised
B. Open a ticket informing the development team about the alerts
C. Check if temporary files are being monitored
D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: C

Explanation:
The analyst should check if temporary files are being monitored first to respond to the issue. Temporary files are files that are created and used by applications for various purposes, such as storing data temporarily or caching data for faster access. However, temporary files are not meant to be permanent and are usually deleted when they are no longer needed or when the application is closed. Therefore, monitoring temporary files can generate many alerts from the file-integrity monitoring tool that are not relevant or useful for security purposes. The analyst should check if temporary files are being monitored and exclude them from the monitoring scope to reduce the number of alerts and focus on the files that should not change.

NEW QUESTION 37
Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?

```
* SSL 3.0 Cipher Suites:
Attempted to connect using 80 cipher suites.
The server accepted the following 10 cipher suites:
TLS_RSA_WITH_RC4_128_SHA 128
TLS_RSA_WITH_RC4_128_MD5 128
TLS_RSA_WITH_DES_CBC_SHA 56
TLS_RSA_WITH_AES_256_CBC_SHA 256
TLS_RSA_WITH_AES_128_CBC_SHA 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA 168

* TLS 1.0 Cipher Suites:
Attempted to connect using 80 cipher suites.
The server accepted the following 10 cipher suites:
TLS_RSA_WITH_RC4_128_SHA 128
TLS_RSA_WITH_RC4_128_MD5 128
TLS_RSA_WITH_DES_CBC_SHA 56
TLS_RSA_WITH_AES_256_CBC_SHA 256
TLS_RSA_WITH_AES_128_CBC_SHA 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA 168
TLS_DHE_RSA_WITH_DES_CBC_SHA 56 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)
The group of cipher suites supported by the server has the following properties:
Forward Secrecy OK - Supported
Legacy RC4 Algorithm INSECURE - Supported
```

A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_WITH_AES_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)

Answer: B

Explanation:
The line from this output that most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key is TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits). This line indicates that the cipher suite uses Diffie-Hellman ephemeral (DHE) key exchange with RSA authentication, AES 128-bit encryption with cipher block chaining (CBC) mode, and SHA-1 hashing. The DHE key exchange uses a 1024-bit Diffie-Hellman group, which is considered too weak for modern security standards and can be broken by attackers using sufficient computing power. The other lines indicate stronger cipher suites that use longer key lengths or more secure algorithms. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9;

https://learn.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

NEW QUESTION 38
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.
D. Remove the application from production and Inform the users.

Answer: B

Explanation:
A routine vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or
network using automated tools or software3
A vulnerability scan does not necessarily mean that there is an active threat or exploit on the system or network, but rather that there are potential weaknesses that could be exploited by attackers. The best next step after a routine vulnerability scan detected a known vulnerability in a critical enterprise web application is to evaluate the risk and criticality of the vulnerability, which means assessing the likelihood and impact of an exploit on the web application, and prioritizing the remediation actions based on the severity and urgency of the vulnerability.

NEW QUESTION 42
A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

A. Deploy an edge firewall.
B. Implement DLP
C. Deploy EDR.
D. Encrypt the hard drives

Answer: B

Explanation:
DLP, or Data Loss Prevention, is a cybersecurity solution that detects and prevents data breaches. It blocks the extraction of sensitive data and prevents the unauthorized or inappropriate sharing, transfer, or use of data. It also helps organizations comply with data protection regulations and policies1
DLP can help defend against sensitive data exfiltration by monitoring and controlling data movement across networks, devices, applications, and cloud services. DLP can also alert or block users from sending or uploading sensitive data to untrusted destinations or recipients.

NEW QUESTION 44
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_inf();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.
B. Implement float numbers instead of integers to prevent integer overflows.
C. Use built-in functions from libraries to check and handle long numbers properly.
D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

Answer: C

Explanation:
The security analyst should implement a control that uses built-in functions from libraries to check and handle long numbers properly. This will help prevent integer overflow vulnerabilities, which occur when a value is moved into a variable type too small to hold it. For example, if an integer variable can only store values up to 255, and a value of 256 is assigned to it, the variable will overflow and wrap around to 0. This can cause unexpected program behavior or lead to buffer overflow vulnerabilities if the overflowed value is used as an index or size for memory allocation1. Built-in functions from libraries can help avoid integer overflow by performing checks on the input values and the resulting values, and throwing exceptions or errors if they exceed the limits of the variable type2.

NEW QUESTION 48
Which of the following data exfiltration discoveries would most likely require communicating a breach to regulatory agencies?

A. CRM data
B. PHI files
C. SIEM logs
D. UEBA metrics

Answer: B

Explanation:
PHI stands for protected health information, which is any information that relates to the health or health care of an individual and can be used to identify that person. PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which sets national standards for the privacy and security of health information. HIPAA requires covered entities, such as health care providers, health plans, and health care clearinghouses, to notify individuals and regulatory agencies of any breach of unsecured PHI. A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of the information

NEW QUESTION 53
An organizational policy requires one person to input accounts payable and another to do accounts receivable. A separate control requires one person to write a check and another person to sign all checks greater than $5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

A. Segregation of duties
B. Job rotation
C. Non-repudiaton
D. Dual control

Answer: A

Explanation:
Segregation of duties is a security control that requires multiple people to be involved with completing a task. This helps prevent fraud, as it ensures that no one individual has the ability to commit fraud or make mistakes without other people being aware of it

NEW QUESTION 56
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

A. Infrastructure
B. Capabilities
C. Adversary
D. Victims

Answer: A

Explanation:
The Diamond Model of Intrusion Analysis is a framework for analyzing and understanding malicious activity on a system or network. It defines the basic atomic element of any intrusion activity as the event, which
consists of four core features: adversary, infrastructure, capability, and victim. These features are connected by edges that represent their underlying relationships and arranged in the shape of a diamond1
The infrastructure feature refers to the physical or logical communication structures that are used by the adversary to deliver a capability or interact with a victim. Examples of infrastructure elements are IP addresses, domain names, email addresses, servers, routers, etc. The domain, IP address, email address, and software version that the analyst extracted from the artifacts are all examples of infrastructure elements that can be used to identify or track the adversary's activity.

NEW QUESTION 59
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system
B. DNS sinkholing
C. IP address allow list
D. An inline IDS

Answer: B

Explanation:
DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole

NEW QUESTION 60
A security is reviewing a vulnerability scan report and notes the following finding:

Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.

Answer: D

Explanation:
The vulnerability scan report shows that the workstation has a high-risk vulnerability (CVE-2019-0708) that affects Remote Desktop Services on Windows systems. This vulnerability allows remote code execution without authentication or user interaction, and can be exploited by sending specially crafted requests to the target system1
As part of the detection and analysis procedures, the analyst should confirm the workstation's
signatures against the most current signatures. This can help verify if the workstation has been patched or updated to address the vulnerability, or if it is still vulnerable and needs remediation. The analyst can use tools such as Windows Update or Microsoft Baseline Security Analyzer to check the workstation's patch level and compare it with the latest available signatures.

NEW QUESTION 65
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: C

Explanation:
Lessons learned is a critical stage of incident response that involves evaluating the effectiveness of the response, identifying gaps and areas for improvement, and updating the incident response plan accordingly1.
Company leadership should be involved in this process to ensure they are aware of the incident, its impact, and the actions taken to prevent or mitigate future incidents. Additionally, company leadership can provide support and guidance for implementing the recommendations from the lessons learned session2.

NEW QUESTION 70
A security analyst works for a biotechnology lab that is planning to release details about a new cancer treatment. The analyst has been instructed to tune the SIEM softvare and IPS in preparation for the
announcement. For which of the following concerns will the analyst most likely be monitoring?

A. Intellectual property loss
B. PII loss
C. Financial information loss
D. PHI loss

Answer: A

Explanation:
SIEM software is a tool that provides a single centralized platform for the collection, monitoring, and management of security-related events and log data from across the enterprise1. SIEM software can help security analysts detect, investigate, and respond to threats, as well as comply with regulations and standards.
IPS stands for Intrusion Prevention System. It is a device or software that monitors network traffic and blocks or modifies malicious packets before they reach their destination2. IPS can help security analysts prevent attacks, protect sensitive data, and reduce network downtime.
A security analyst working for a biotechnology lab that is planning to release details about a new cancer treatment would most likely be monitoring for A. Intellectual property loss. Intellectual property (IP) refers t the creations of the mind, such as inventions, designs, artistic works, or trade secrets3. IP loss occurs when someone steals, leaks, or misuses the IP of an organization without authorization.
The biotechnology lab's new cancer treatment is an example of IP that has high value and potential impact on the market and society. Therefore, the security analyst would want to protect it from competitors, hackers, or other malicious actors who might try to access it illegally or sabotage it. The security analyst would use SIEM software and IPS to monitor for any signs of unauthorized access, data exfiltration, or tampering with the lab's network or systems.

NEW QUESTION 72
A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:

```
Source: Email filtering tool
Event: Malicious message delivered notification
ID: 1905

Source: Antivirus Solution
Event: Virus CS0-726 detected
ID: 2008

Source: Firewall
Event: Outbound connection to known-bad IP blocked
ID: 1987
```

Which of the following is the best way for the analyst to automate alert generation?

A. Deploy a signature-based IDS
B. Install a UEBA-capable antivirus
C. Implement email protection with SPF
D. Create a custom rule on a SIEM

Answer: D

Explanation:
A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15;
https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-impleme

NEW QUESTION 77
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

A. Critical asset list
B. Threat vector
C. Attack profile
D. Hypothesis

Answer: D

Explanation:
A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific question to answer, such as “Is there any evidence of lateral movement within our network?” or “Are there any signs of data exfiltration from our servers?”.

NEW QUESTION 81
An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the malware analysis process
B. Consult the disaster recovery plan
C. Consult the data classification process
D. Consult the communications plan

Answer: D

Explanation:
A communications plan is a document that outlines who should be notified and how during an incident response. It can also specify the roles and responsibilities of the incident response team members, the escalation procedures, and the communication channels. Consulting the communications plan is the most appropriate next step in an incident response plan after determining a security incident has occurred. Consulting the malware analysis process, the disaster recovery plan, or the data classification process may be relevant at later stages of the incident response, but not as the next step. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 86
During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?

A. Consult with the legal department for regulatory impact.
B. Encrypt the database with available tools.
C. Email the customers to inform them of the breach.
D. Follow the incident communications process.

Answer: D

Explanation:
An incident communications process is a set of procedures that defines how to communicate with internal and external stakeholders during and after an incident, such as customers, employees, management, regulators and media. An incident communications process can help to provide accurate, timely and consistent information about the incident, its impact and the actions taken to resolve it. An incident communications process can also help to maintain trust and reputation, comply with legal obligations and prevent misinformation or confusion3.

NEW QUESTION 87
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Set up an FTP server that both companies can access and export the required financial data to a folder.
B. Set up a VPN between Company A and Company
C. granting access only lo the ERPs within theconnection
D. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
E. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

Answer: C

Explanation:
The security analyst should set up a PKI (Public Key Infrastructure) between Company A and Company B and exchange shared certificates between the two entities. This will allow them to establish a more automated approach to secure data transfers between their ERP systems. A PKI is a system that provides encryption and authentication services using public key cryptography. A PKI consists of certificates, certificate authorities (CAs), and other components that enable users to securely exchange data over untrusted networks. By exchanging shared certificates between Company A and Company B, they can verify each other’s identity and encrypt their data using public and private keys.

NEW QUESTION 89
A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:

Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(#ros.println(31337*31337)).(#ros.flush())}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center: X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

Winch of the following actions should the security analyst lake NEXT?

A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
B. Contact the application owner for connect example local tor additional information
C. Mark the alert as a false positive scan coming from an approved source.
D. Raise a request to the firewall team to block 203.0.113.15.

Answer: A

Explanation:
The security analyst should review the known Apache vulnerabilities to determine if a compromise actually occurred. The SIEM alert indicates that an IDS signature detected an attempt to exploit a vulnerability in Apache Struts 2 (CVE-2017-5638), which allows remote code execution via a crafted Content-Type header4. The packet capture and TCP stream show that the attacker sent a malicious request with a Content-Type header containing an OGNL expression that executes the command “whoami” on the target server. However, this does not necessarily mean that the attack was successful, as it depends on whether the target server was running a vulnerable version of Apache Struts 2 or not. Therefore, the security analyst should review the known Apache vulnerabilities and compare them with the version of Apache Struts 2 running on the server to confirm if a compromise actually occurred or not.

NEW QUESTION 92
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

A. Perform an assessment of the firmware to determine any malicious modifications.
B. Conduct a trade study to determine if the additional risk constitutes further action.
C. Coordinate a supply chain assessment to ensure hardware authenticity.
D. Work with IT to replace the devices with the known-altered motherboards.

Answer: C

Explanation:
A supply chain assessment is a process that evaluates the security and integrity of the suppliers and vendors that provide hardware or software to an organization. It can help identify and mitigate the risk of tampered or counterfeit products that could compromise the organization’s security or performance. Coordinating a supply chain assessment to ensure hardware authenticity is the best course of action to mitigate the risk of motherboards that have been physically altered during the manufacturing process. Performing an assessment of the firmware, conducting a trade study, or working with IT to replace the devices are other possible actions, but they are not as effective or proactive as coordinating a supply chain assessment. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-161.pdf

NEW QUESTION 97
An organization completed an internal assessment of its policies and procedures. The audit team identified a deficiency in the policies and procedures for PH. Which of the following should be the first step to secure the organization's Pll?

A. Complete Pll training within the organization.
B. Contact all Pll data owners within the organization.
C. Identify what type of Pll is on the network.
D. Formalize current Pll documentation.

Answer: C

Explanation:
Pll stands for Personally Identifiable Information, and it is any data that can be used to identify, locate, or contact an individual. Examples of Pll include names, addresses, phone numbers, email addresses, social security numbers, bank account numbers, etc. The first step to secure the organization’s Pll is to identify what type of Pll is on the network, where it is stored, who has access to it, and how it is transmitted. This can help determine the scope and impact of the deficiency in the policies and procedures for Pll.

NEW QUESTION 98
A security analyst is reviewing vulnerability scans from an organization's internet-facing web services. The following is from an output file called ssl-test_webapps.comptia.org:

```
SCAN RESULTS FOR webapps.comptia.org:443 - 52.165.16.154
---------------------------------------------------------
* Certificates Information:
Hostname sent for SNI: webapps.comptia.org
Number of certificates detected: 1

Certificate #0 ( _RSAPublicKey )
SHA1 Fingerprint: 44175dea3a5b1a21fb94698072b3427bf4607117
Common Name: *.comptia.org
Public Key Algorithm: _RSAPublicKey
Signature Algorithm: sha256
Key Size: 2048
Exponent: 65537
DNS Subject Alternative Names: ['*.comptia.org']


Certificate #0 - Extensions
OCSP Must-Staple: NOT SUPPORTED - Extension not found
Certificate Transparency: OK - 3 SCTs included
Certificate #0 - OCSP Stapling
NOT SUPPORTED - Server did not send back an OCSP response


* TLS 1.0 Cipher Suites:
Attempted to connect using 80 cipher suites.
The server accepted the following 10 cipher suites:
TLS_RSA_WITH_RC4_128_SHA 128
TLS_RSA_WITH_RC4_128_MD5 128
TLS_RSA_WITH_DES_CBC_SHA 56
TLS_RSA_WITH_AES_256_CBC_SHA 256
TLS_RSA_WITH_AES_128_CBC_SHA 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA 168
TLS_DHE_RSA_WITH_DES_CBC_SHA 56 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)
The group of cipher suites supported by the server has the following properties:
Forward Secrecy OK - Supported
Legacy RC4 Algorithm INSECURE - Supported
```

Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?

A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_K1TH_A£S_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)

Answer: A

Explanation:
This line from the output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key, as it represents a weak cipher suite that uses an outdated encryption algorithm, a small key size, and no forward secrecy. A cipher suite is a combination of cryptographic algorithms and parameters that are used to establish a secure communication channel between two parties. The cipher suite in this line consists of four components: TLS_RSA_WITH_DES_CBC_SHA 56.

- TLS stands for Transport Layer Security, and it is a protocol that provides security and privacy for network communications.
- RSA stands for Rivest-Shamir-Adleman, and it is an algorithm that uses public-key cryptography for key exchange and authentication.
- DES stands for Data Encryption Standard, and it is an algorithm that uses symmetric-key cryptography for data encryption.
- CBC stands for Cipher Block Chaining, and it is a mode of operation that encrypts each block of data by XORing it with the previous ciphertext block.
- SHA stands for Secure Hash Algorithm, and it is an algorithm that produces a fixed-length hash value from any input data.
- 56 stands for the key size in bits, which indicates how strong or secure the encryption is.

The cipher suite in this line is weak because:

- DES is an outdated encryption algorithm that has been broken by brute force attacks, as it has a small key size of 56 bits, which can be easily guessed by modern computers.
- RSA does not provide forward secrecy, which means that if the RSA private key is compromised, all past and future communications encrypted with that key can be decrypted by an attacker.
- SHA is also an outdated hash algorithm that has been replaced by newer versions such as SHA-2 or SHA-3, as it has some vulnerabilities and weaknesses.

NEW QUESTION 99
An analyst is performing a BIA and needs to consider measures and metrics. Which of the following would help the analyst achieve this objective? (Select two).

A. Time to reimage the server
B. Minimum data backup volume
C. Disaster recovery plan for non-critical services
D. Maximum downtime before impact is unacceptable
E. Time required to inform stakeholders about outage
F. Total time accepted for business process outage

Answer: DF

Explanation:
The objective of a BIA is to determine the potential impacts of various disruptions on the business processes and functions, and to establish the recovery priorities and objectives for each process and function. To achieve this objective, the analyst needs to consider various measures and metrics that can quantify the impacts

and the recovery requirements. Some of the common measures and metrics that are used in a BIA are:

- Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD). It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption1.
- Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month. This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption1. It helps to determine the backup frequency and retention policy for the data and systems that support the process or function.
- Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function. This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption2. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.
- Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications. It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare3.
- Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption. It also helps to identify the critical data elements and sources that are essential for the process or function4.

NEW QUESTION 100
Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Answer: B

Explanation:
SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope. SOAR (Security Orchestration, Automation and Response) is a technology that helps coordinate, execute and automate tasks between various people and tools within a single platform. SOAR can help improve the efficiency and effectiveness of security operations by reducing manual effort, enhancing
collaboration, and accelerating incident response1. SCAP (Security Content Automation Protocol) is a standard that enables automated vulnerability management, measurement and policy compliance evaluation of systems deployed in an organization2. SCAP can help assess the security posture and compliance status of systems by using predefined specifications and checklists. However, SCAP does not provide orchestration or automation capabilities beyond vulnerability scanning and reporting.

NEW QUESTION 104
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance.
B. Implement blacklisting lor IP addresses from outside the county.
C. Implement strong authentication controls for at contractors.
D. Implement user behavior analytics tor key staff members.

Answer: A

Explanation:
A secure supply chain program is a set of processes and practices that aim to protect the supply chain from various risks, such as cyberattacks, data breaches, fraud, theft, sabotage, or natural disasters1. A secure supply chain program can help to ensure the integrity, availability, and confidentiality of the products, services, data, and systems involved in the supply chain. A secure supply chain program with governance means that there are clear roles, responsibilities, policies, procedures, and controls for managing the security of the supply chain. This can help to monitor and enforce the compliance of the third-party service provider with the requirement to source talent from its own country. A secure supply chain program with governance can also help to identify and mitigate any potential threats or vulnerabilities in the supply chain. Implementing blacklisting for IP addresses from outside the country (B) may not be sufficient or effective, as IP addresses can be spoofed or bypassed by attackers. Implementing strong authentication controls for all contractors © may not be relevant or adequate, as authentication controls do not prevent the sourcing of talent from other countries. Implementing user behavior analytics for key staff members (D) may not be applicable or useful, as user behavior analytics do not verify the origin or location of the talent.

NEW QUESTION 109
A Chief Information Security Officer has requested a security measure be put in place to redirect certain traffic on the network. Which of the following would best resolve this issue?

A. Sinkholing
B. Blocklisting
C. Geoblocking
D. Sandboxing

Answer: A

Explanation:
Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to a server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1.
For example, sinkholing can be used to redirect traffic from a botnet or a malware-infected host to a server under the control of the defender, where the traffic can

be analyzed, blocked, or neutralized. This can help identify and isolate compromised devices, prevent command-and-control communication, and disrupt malicious activities2.
The other options are not the best solutions for the following reasons:

- Blocklisting is a technique for preventing access to or communication with certain IP addresses, domains, or applications that are known or suspected to be malicious. Blocklisting can be implemented using firewalls, routers, proxies, or software tools. Blocklisting can protect a network from unwanted or harmful traffic, but it does not redirect the traffic to a different destination.
- Geoblocking is a technique for restricting access to or communication with certain IP addresses, domains, or applications based on their geographic location. Geoblocking can be implemented using firewalls, routers, proxies, or software tools. Geoblocking can protect a network from unauthorized or undesirable traffic from specific regions or countries, but it does not redirect the traffic to a different destination.
- Sandboxing is a technique for isolating and executing potentially malicious code or applications in a separate and secure environment. Sandboxing can be implemented using virtual machines, containers, or software tools. Sandboxing can protect a network from malware infection or damage, but it does not redirect the network traffic to a different destination.

NEW QUESTION 113
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

A. Network
B. Physical
C. Adjacent
D. Local

Answer: C

Explanation:
The Common Vulnerability Scoring System (CVSS) is a standard for measuring the severity of vulnerabilities in software systems. One of the factors that affects the CVSS score is the attack vector, which describes how the vulnerability can be exploited. The possible values for the attack vector are network, adjacent network, local, or physical. In this case, the analyst should choose local as the value for the attack vector, because the Tomcat configuration file must be modified for the attack to be successful, which implies that the attacker needs local access to the system. Network, adjacent network, or physical are not appropriate values for the attack vector in this scenario. Reference:
https://www.first.org/cvss/v3.1/specification-document#Vector-String

NEW QUESTION 115
An organization is required to be able to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams. The organization would also like to be able to leverage the intelligence to enrich security event data. Which of the following functions would most likely help the security analyst meet the organization's requirements?

A. Vulnerability management
B. Risk management
C. Detection and monitoring
D. Incident response

Answer: C

Explanation:
The correct answer is C. Detection and monitoring. Detection and monitoring is a function that involves collecting, analyzing, and correlating data from various sources, such as threat feeds, logs, alerts, or events, to identify and respond to potential or ongoing threats. Detection and monitoring can help the organization to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams, such as security operations center (SOC) analysts, incident responders, or threat hunters. Detection and monitoring can also help the organization to leverage the intelligence to enrich security event data, such as adding context, severity, or priority to the events1.
* A. Vulnerability management is not correct. Vulnerability management is a function that involves identifying, assessing, and mitigating the weaknesses or flaws in systems, applications, or networks that could be exploited by attackers. Vulnerability management can help the organization to reduce its attack surface and prevent potential breaches, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* B. Risk management is not correct. Risk management is a function that involves identifying, analyzing, and evaluating the risks that could affect the organization’s assets, operations, or objectives. Risk management can help the organization to prioritize and implement appropriate controls or mitigation strategies to reduce the likelihood or impact of the risks, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* D. Incident response is not correct. Incident response is a function that involves preparing for, detecting, containing, analyzing, and recovering from security incidents that compromise the confidentiality, integrity, or availability of the organization’s assets or operations. Incident response can help the organization to minimize the damage and restore normal operations as quickly as possible, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
1: Cybersecurity Analyst+ - CompTIA

NEW QUESTION 120
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.
B. decode.
C. guess.
D. decrypt.

Answer: B

Explanation:
Lime-based cookies are a type of cookies that use lime encoding to store data in a web browser. Lime
encoding is a simple substitution cipher that replaces each character in a string with another character based on a fixed key. Lime-based cookies are easy to decode because the key is publicly available and the encoding algorithm is simple. Anyone who intercepts or accesses the lime-based cookies can easily decode them and read the data stored in them. This is a security concern because lime-based cookies are often used for session management, which means they store

information about the user's identity and preferences on a web application. If an attacker can decode the lime-based cookies, they can impersonate the user or access their sensitive information.

NEW QUESTION 124
An organization has a policy that requires dedicated user accounts to run programs that need elevated privileges. Users must be part of a group that allows elevated permissions. While reviewing security logs, an analyst sees the following:

PRI	TIME	HOST	MESSAGE
34	Oct 22 10:01:33	lincoln	'su root' failed for ldavis on /dev/pts/8
38	Oct 22 11:01:45	ford	'sudo apache.bin' failed for ldavis on /dev/sda
34	Oct 22 13:32:18	gremlin	'sudo more /etc/passwd' failed for ldavis on /dev/hda
30	Oct 22 15:27:19	pacer	'more /etc/passwd' failed for ldavis on /dev/hda

Which of the following hosts violates the organizational policies?

A. pacer
B. ford
C. gremlin
D. lincoln

Answer: D

Explanation:
The host "lincoln" violates the organizational policies that require dedicated user accounts to run programs that need elevated privileges. The log file shows that the user "ldavis" tried to run programs such as "su root", "sudo apache.bin", and "sudo grep" on the host "lincoln", which indicate attempts to gain elevated privileges or access sensitive files. The other hosts do not show any evidence of policy violation.

NEW QUESTION 128
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is compatia.org. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

A. Add TXT @ "v=spfl mx include:_spf.compti
B. org -all" to the DNS record.
C. Add : XT @ "v=spfl mx include:_sp£.comptia.org -all" to the email server.
D. Add TXT @ "v=spfl mx include:_sp£.comptia.org +all" to the domain controller.
E. AddTXT @ "v=apfl mx lnclude:_spf .comptia.org +a 11" to the web server.

Answer: A

Explanation:
Adding TXT @ "v=spfl mx include:_spf.comptia. org -all" to the DNS record can help to prevent outside entities from spoofing the company's email domain, which is comptia.org. This is an example of a Sender Policy Framework (SPF) record, which is a type of DNS record that specifies which mail servers are authorized to send email on behalf of a domain. SPF records can help to prevent spoofing by allowing the recipient mail servers to check the validity of the sender's domain against the SPF record. The "-all" at the end of the SPF record indicates that any mail server that is not listed in the SPF record is not authorized to send email for comptia.org .

NEW QUESTION 133
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:

A. the responder's discretion.
B. the public relations policy.
C. the communication plan.
D. the senior management team's guidance.

Answer: C

Explanation:
The communication plan is an important part of incident response, as it outlines how and when information about the incident should be shared with external entities.
A communication plan is a set of procedures and protocols that define how an organization should communicate with external entities during times of emergency or security incident. The plan typically outlines how and when information about the incident should be shared, and ensures that any relevant stakeholders are informed of the incident in a timely manner. It also serves as a guide for determining what information to share with outside parties. Here is a link to an article from CompTIA's website about the importance of a communication plan for incident response for your reference:
https://www.comptia.org/content/incident-response-communication-plan

NEW QUESTION 134
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

A. Physical key
B. Retinal scan
C. Passphrase
D. Fingerprint

Answer: B

Explanation:
A retinal scan is a biometric authentication method that uses the unique pattern of blood vessels in the retina to verify a person's identity. It is considered a strong and reliable authentication method that would enhance the datacenter's security. A physical key, a passphrase, or a fingerprint are other authentication methods, but they are not as secure or reliable as a retinal scan. Reference:
https://www.techopedia.com/definition/2586/retinal-scan

NEW QUESTION 139
A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: D

Explanation:
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You're only worried about that if you're in multiple locations. .
https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally
Geographic access requirements are an appropriate technical control to implement to mitigate data sovereignty issues. Data sovereignty issues arise when data is subject to different laws and regulations depending on where it is stored or processed. For example, some countries may have stricter data protection or privacy laws than others, or may impose restrictions on cross-border data transfers. Geographic access requirements can help ensure that data is only accessed from locations that comply with the applicable laws and regulations, and prevent unauthorized access from locations that do not.

NEW QUESTION 143
Which of following allows Secure Boot to be enabled?

A. eFuse
B. UEFI
C. MSM
D. PAM

Answer: B

Explanation:
UEFI, or Unified Extensible Firmware Interface, is a specification that defines the software interface between an operating system and platform firmware. UEFI replaces the legacy BIOS (Basic Input/Output System) interface that was used to boot and configure computers. UEFI provides several advantages over BIOS, such as faster boot times, better security features, larger disk support, graphical user interface, etc. One of the security features that UEFI supports is Secure Boot, which is a mechanism that ensures that only authorized software can run during the boot process. Secure Boot prevents unauthorized or malicious code from loading or executing before the operating system starts. Secure Boot works by verifying the digital signature of each piece of boot software against a database of trusted keys stored in UEFI firmware. If the signature is valid, the software is allowed to run; otherwise, it is blocked or rejected.

NEW QUESTION 147
A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.
B. Develop a query to search for the indicators of compromise.
C. Develop a new signature to alert on the indicators of compromise.
D. Develop a new signature to block the indicators of compromise.

Answer: B

Explanation:
Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the environment and initiate further investigation or response .

NEW QUESTION 149
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr
0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr
0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val
719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length
0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length
0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr
0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59809 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
```

Which of the following generated the above output?

A. A port scan
B. A TLS connection
C. A vulnerability scan
D. A ping sweep

Answer: B

Explanation:
A port scan generated the output. A port scan is a type of attack that probes a host or a network for open ports or services. A port scan can help an attacker discover potential vulnerabilities or entry points for further exploitation. The output shows that tcpdump captured packets with different flags, such as SYN, ACK, RST, and FIN, which indicate different stages of the TCP three-way handshake or connection termination. The output also shows that the source IP address 192.168.1.100 sent packets to different destination ports on the target IP address 192.168.1.101, such as 22, 23, 25, 80, and 443. These are common ports that an attacker would scan to find out what services are running on the target.

NEW QUESTION 150
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

A. STIX
B. OpenlOC
C. CVSS
D. TAXll

Answer: D

Explanation:
TAXII stands for Trusted Automated eXchange of Indicator Information, and it is a server component of a threat management system that can facilitate the exchange of threat intelligence data between different sources and consumers, using a standard protocol and format. TAXII can help deploy a threat management system with minimal human interaction, by automating the collection, processing, and dissemination of threat intelligence data.

NEW QUESTION 151
A security analyst discovers suspicious activity going to a high-value corporate asset. After reviewing the traffic, the security analyst identifies that malware was successfully installed on a machine. Which of the following should be completed first?

A. Create an IDS signature of the malware file.
B. Create an IPS signature of the malware file.
C. Remove the malware from the host.
D. Contact the systems administrator.

Answer: C

Explanation:
According to the CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives1, one of the skills required for the exam is to “apply incident response procedures and analyze potential indicators of
compromise (IOCs)”. The document also states that “the first step in incident response is to contain the incident and prevent further damage” (page 14).
Based on this information, the best answer to your question is C. Remove the malware from the host. This would prevent the malware from spreading to other machines or exfiltrating data from the infected host.

NEW QUESTION 155
An analyst reviews a legacy Windows XP system and concludes an attacker executed code that modified the contents of the system's memory. Which of the following attack techniques did the attacker use?

A. Rootkit
B. Backdoor
C. Privilege escalation
D. Buffer overflow

Answer: D

Explanation:
A buffer overflow is an attack technique that exploits a vulnerability in a program's memory management, by sending more data than the buffer can hold. This can cause the program to overwrite adjacent memory locations, and execute arbitrary code injected by the attacker.

NEW QUESTION 160
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications

Answer: D

Explanation:
Blocking third-party applications would be the best way to mitigate future attacks on company-owned mobile devices that are used by employees to collect data from clients in the field. Third-party applications are applications that are not developed or authorized by the device manufacturer or operating system provider1. Third-party applications can pose a security risk for mobile devices, as they may contain malware, spyware, or other malicious code that can compromise the device or its data2. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

NEW QUESTION 162
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?

A. Require users to sign NDAs
B. Create a data minimization plan.
C. Add access control requirements.
D. Implement a data loss prevention solution.

Answer: B

Explanation:
A data minimization plan is a strategy that aims to reduce the amount and type of data that an organization collects, stores, and processes. It can help improve data privacy and protection by limiting the exposure and impact of a data breach or loss. Creating a data minimization plan is the best recommendation for a security officer who needs to find the most cost-effective solution to the current data privacy and protection gap. Requiring users to sign NDAs, adding access control requirements, or implementing a data loss prevention solution are other possible solutions, but they are not as cost-effective as creating a data minimization plan. Reference:
https://www.csoonline.com/article/3603898/data-minimization-what-is-it-and-how-to-implement-it.html

NEW QUESTION 164
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members

Answer: A

Explanation:
Implementing a secure supply chain program with governance would be the best way to ensure the third-party service provider meets the requirement of only sourcing talent from its own country. A secure supply chain program is a set of policies, procedures, and controls that aim to protect the integrity and security of the products and services delivered by third-party vendors. A secure supply chain program can help mitigate the risks of geopolitical and national security interests by verifying the origin, identity, and trustworthiness of the vendors and their employees1. Governance is a key component of a secure supply chain program, as it provides oversight, accountability, and enforcement of the policies and procedures.

NEW QUESTION 168
A forensic examiner is investigating possible malware compromise on an active endpoint device. Which of the following steps should the examiner perform first?

A. Verify the hash value of the image with the value of the copy.
B. Use a write blocker to create an image of the hard drive.
C. Create a memory dump from RAM.
D. Download and apply the latest AV signature.
E. Reimage the hard drive and apply the latest updates.

Answer: C

Explanation:
A memory dump is a snapshot of the contents of the random access memory (RAM) of a system at a given
point in time. A memory dump can provide valuable information for a forensic examiner who is investigating possible malware compromise on an active endpoint device, such as running processes, open files, network connections, encryption keys, or malware artifacts. Creating a memory dump from RAM should be the first

step that the examiner performs, as it preserves the volatile data that could be lost or altered if the system is powered off or rebooted1.

NEW QUESTION 171
An organization is performing a risk assessment to prioritize resources for mitigation and remediation based on impact. Which of the following metrics, in addition to the CVSS for each CVE, would best enable the organization to prioritize its efforts?

A. OS type
B. OS or application versions
C. Patch availability
D. System architecture
E. Mission criticality

Answer: C

Explanation:
A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect an organization's assets, operations, or objectives. A risk assessment matrix is a tool that can help prioritize the risks based on their likelihood and impact1.
The CVSS (Common Vulnerability Scoring System) is a standard framework for rating the severity of vulnerabilities in software systems. The CVSS provides a numerical score from 0 to 10, as well as a qualitative rating from Low to Critical, based on the characteristics and consequences of the vulnerability2.
However, the CVSS score alone may not be sufficient to determine the priority of mitigation and remediation actions for each vulnerability. Other factors that may influence the decision include:

- Patch availability: This metric indicates whether there is a fix or update available for the vulnerability from the vendor or developer. Patch availability can affect the urgency and feasibility of remediation, as well as the risk exposure and potential damage of exploitation. For example, a vulnerability with a high CVSS score but with a readily available patch may be less critical than a vulnerability with a lower CVSS score but with no patch available3.
- Mission criticality: This metric reflects the importance and value of the asset or system affected by the vulnerability to the organization's mission, goals, or functions. Mission criticality can affect the impact and priority of remediation, as well as the risk tolerance and acceptance level of the organization. For example, a vulnerability with a high CVSS score but affecting a non-essential system may be less critical than a vulnerability with a lower CVSS score but affecting a core system4.
- OS type: This metric indicates the operating system (OS) of the asset or system affected by the vulnerability. OS type can affect the likelihood and complexity of exploitation, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an uncommon or unsupported OS may be less critical than a vulnerability with a lower CVSS score but affecting a widely used or supported OS3.
- OS or application versions: This metric indicates the specific version of the OS or application affected by the vulnerability. OS or application versions can affect the applicability and relevance of the vulnerability, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an outdated or obsolete version may be less critical than a vulnerability with a lower CVSS score but affecting a current or popular version3.
- System architecture: This metric indicates the design and configuration of the asset or system affected by the vulnerability. System architecture can affect the exposure and accessibility of the vulnerability, as well as the effectiveness and efficiency of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an isolated or segmented system may be less critical than a vulnerability with a lower CVSS score but affecting an interconnected or integrated system3.

Therefore, to best enable the organization to prioritize its efforts based on impact, patch availability is one of the most important metrics to consider in addition to the CVSS score for each CVE (Common Vulnerabilities and Exposures). Patch availability can directly influence the risk level and remediation strategy for each vulnerability.

NEW QUESTION 172
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. SAST
C. DAST
D. DACS

Answer: A

Explanation:
SCAP is a protocol designed to assess the security compliance of computers and other devices. It works by scanning systems against security policies, and can help verify that the scanned device meets security requirements. Here is a link to the CompTIA CySA+ Guide's Chapter 5 - Access Controls for more information: https://certification.comptia.org/docs/default-source/exam-objectives/cs0-002.pdf

NEW QUESTION 176
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
Which of the following most likely occurred?

A. The attack used an algorithm to generate command and control information dynamically.
B. The attack attempted to contact www.google.com to verify internet connectivity.
C. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
D. The attack caused an internal host to connect to a command and control server.

Answer: A

Explanation:
This is a technique that is commonly used by malware to evade detection and blocking by security tools. The malware generates random domain names that are used to communicate with the command and control server, which can change its IP address frequently. The domain names are usually long and nonsensical, such as www.uewiryfajfchfaerwfj.co in the log. The malware uses a predefined algorithm or a seed value to generate the same domain names as the server, so that they can find each other on the internet12.

NEW QUESTION 180
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?

A. Asset tagging
B. SIEM
C. File integrity monitor
D. DLP

Answer: D

Explanation:
DLP (Data Loss Prevention) is what the CISO wants to purchase. DLP is a solution that prevents unauthorized or accidental disclosure of sensitive data by monitoring, detecting, and blocking data transfers or downloads that violate predefined policies or rules3. DLP can also track and classify data assets based on various criteria, such as name, type, content, or data profile4. DLP can help protect data from insider threats, external attackers, or human errors.

NEW QUESTION 185
industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control

Answer: D

Explanation:
Role-based access control (RBAC) is a method of restricting access to resources based on the roles of users within an organization. RBAC assigns permissions and privileges to roles, rather than individual users, and grants access based on the principle of least privilege3
RBAC can help mitigate the risk of privilege escalation attacks on SCADA devices by ensuring that only authorized users have access to SCADA administration and management functions, and that they have the minimum level of access required to perform their tasks.

NEW QUESTION 190
A security analyst performed a targeted system vulnerability scan to obtain critical information. After the output result, the analyst used the OVAL XML language to review and calculate the discovered risk. Which of the following types of scans did the security analyst perform?

A. Active
B. Network map
C. Passive
D. External

Answer: A

Explanation:
An active scan is a type of system vulnerability scan that involves sending probes or packets to the target system, and analyzing the responses or behaviors of the system. An active scan can help obtain critical information about the system, such as open ports, running services, operating system, software versions, etc. An active scan can also use OVAL XML language to review and calculate the discovered risk. OVAL stands for Open Vulnerability and Assessment Language, and it is a standard for describing and exchanging information about system vulnerabilities and configurations.

NEW QUESTION 192
A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.
B. Deploy network address protection with DHCP and dynamic VLANs.
C. Configure 802.1X and EAPOL across the network
D. Implement software-defined networking and security groups for isolation

Answer: A

Explanation:
The security analyst should implement port security with one MAC address per network port of the switch. This will help prevent possible physical attacks on the network access layer, such as MAC flooding or MAC spoofing. Port security is a feature that allows a switch to limit the number of MAC addresses that can be learned on a specific port. By setting the limit to one MAC address per port, the switch will only allow traffic from the device that is connected to that port, and drop any traffic from other devices that try to use that
port. This will prevent attackers from connecting unauthorized devices to the network or impersonating
legitimate devices by changing their MAC addresses3.

NEW QUESTION 197

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

Explanation:
The strings command is a Linux utility that can extract human-readable content from any file or partition3. It can be used to analyze a Linux swap partition by finding text strings that may indicate malicious activity or compromise4. The head command (B) can only display the first few lines of a file or partition, which may not contain any useful information. The fsstat command © can only display file system statistics such as size, type, and layout, which may not reveal any human-readable content. The dd command (D) can only copy or convert a file or partition, which may not extract any human-readable content.
References: 3: https://linux.die.net/man/1/strings 4: https://www.linuxjournal.com/content/using-strings-command

NEW QUESTION 198
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
• 20% of the logs are 403
• 20% of the logs are 404
• 50% of the logs are 200
• 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

A. cat access_log Igrep " 403 "
B. cat access_log Igrep " 200 "
C. cat access_log Igrep " 100 "
D. cat access_log Igrep " 4 04 "
E. cat access_log Igrep " 204 "

Answer: B

Explanation:
Requests sent from the same IP address using different user agents are likely to be malicious or suspicious, as they indicate that an attacker is trying to evade detection or bypass security controls by changing their browser or device identification. These requests may indicate that an attacker is using automated tools or scripts to scan or attack the web server.
Requests identified by a threat intelligence service with a bad reputation are also likely to be malicious or suspicious, but they are not the source of the activity, as they originate from different IP addresses. These requests may indicate that an attacker is trying to exploit a vulnerability or perform reconnaissance on the web server.
Requests blocked by the web server per the input sanitization are not likely to be the source of the activity, as they indicate that the web server has successfully prevented an attack by validating and filtering any malicious input from the requests. These requests may indicate that an attacker is trying to inject malicious code or commands into the web server.
Failed log-in attempts against the web application are not likely to be the source of the activity, as they indicate that the web application has successfully prevented unauthorized access by verifying and rejecting any invalid credentials from the requests. These requests may indicate that an attacker is trying to guess or brute-force passwords or usernames for the web application.
Requests sent by NICs with outdated firmware are not likely to be the source of the activity, as they indicate that some devices on the network have not been updated with the latest security patches or features for their network interface cards (NICs). These requests may indicate that some devices are vulnerable to network attacks or have performance issues.
Existence of HTTP/501 status codes generated to the same IP address are not likely to be the source of the activity, as they indicate that the web server has encountered an error or does not support a request method from the client. These requests may indicate that an attacker is trying to use an invalid or unsupported method to access the web server.

NEW QUESTION 203
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

A. Data carving
B. Timeline construction
C. File cloning
D. Reverse engineering

Answer: D

Explanation:
Reverse engineering is a process of analyzing a system or a component to understand how it works and how it was made. Reverse engineering can be used to examine malicious processes captured from memory and determine their functionality, origin, and purpose. Reverse engineering can help identify the type of malware, its infection vector, its capabilities, its communication methods, and its indicators of compromise2

NEW QUESTION 206
Which of the following is the BEST option to protect a web application against CSRF attacks?

A. Update the web application to the latest version.
B. Set a server-side rate limit for CSRF token generation.
C. Avoid the transmission of CSRF tokens using cookies.
D. Configure the web application to only use HTTPS and TLS 1.3.

Answer: C

Explanation:
CSRF tokens are random values that are generated by the server and included in requests that perform state-changing actions. They are used to prevent CSRF attacks by verifying that the request originates from a legitimate source. However, if the CSRF tokens are transmitted using cookies, they are vulnerable to being stolen or forged by an attacker who can exploit other vulnerabilities, such as cross-site scripting (XSS) or cookie injection. Therefore, a better option is to avoid the transmission of CSRF tokens using cookies and use other methods, such as hidden form fields or custom HTTP headers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 11; https://owasp.org/www-community/attacks/csrf

NEW QUESTION 208
A security analyst is designing firewall rules to prevent external IP spoofing Which of the following explains the firewall rule for mitigation?

A. Packets with external source IP addresses do not enter the network from either direction.
B. Packets with internal source IP addresses do not enter the network from the outside.
C. Packets with internal source IP addresses do not exit the network from the inside.
D. Packets with public IP addresses do not pass through the router in either direction.

Answer: B

Explanation:
Packets with internal source IP addresses do not enter the network from the outside. This firewall rule can prevent external IP spoofing, which is an attack technique that involves forging the source IP address of a packet to impersonate another host or network. By blocking packets with internal source IP addresses from entering the network from the outside, the firewall can filter out spoofed packets that claim to originate from the internal network.

NEW QUESTION 210
Members of the sales team are using email to send sensitive client lists with contact information to their personal accounts The company's AUP and code of conduct prohibits this practice. Which of the following configuration changes would improve security and help prevent this from occurring?

A. Configure the DLP transport rules to provide deep content analysis.
B. Put employees' personal email accounts on the mail server on a blocklist.
C. Set up IPS to scan for outbound emails containing names and contact information.
D. Use Group Policy to prevent users from copying and pasting information into emails.
E. Move outbound emails containing names and contact information to a sandbox for further examination.

Answer: A

Explanation:
Data loss prevention (DLP) is a set of policies and tools that aim to prevent unauthorized disclosure of sensitive data. DLP transport rules are rules that apply to email messages that are sent or received by an organization’s mail server. These rules can provide deep content analysis, which means they can scan the content of email messages and attachments for sensitive data patterns, such as client lists or contact information. If a rule detects a violation of the DLP policy, it can take actions such as blocking, quarantining, or notifying the sender or recipient. This would improve security and help prevent sales team members from sending sensitive client lists to their personal accounts. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/data-loss-prevention

NEW QUESTION 214
Which of the following is the primary reason financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector?

A. To augment information about common malicious actors and indicators of compromise
B. To prevent malicious actors from knowing they can defend against malicious attacks
C. To keep other industries from accessing information meant for financial institutions
D. To focus on attacks specifically targeted at their customers’ mobile applications

Answer: A

Explanation:
This is the primary reason why financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector. Threat intelligence is the collection, analysis, and dissemination of information about current or potential threats to an organization’s assets, operations, or reputation. By sharing threat intelligence information, financial institutions can benefit from the collective knowledge, experience, and capabilities of their peers and partners, and enhance their situational awareness, threat detection, and incident response. Sharing threat intelligence information can also help financial institutions identify common attack patterns, trends, and techniques, as well as the malicious actors and indicators of compromise (IOCs) associated with them. IOCs are pieces of forensic data that can be used to identify potentially malicious activities or intrusions on a network or system, such as IP addresses, domains, URLs, file hashes, or email addresses

NEW QUESTION 219
An organization supports a large number of remote users. Which of the following is the best option to protect the data on the remote users' laptops?

A. Require the use of VPNs.
B. Require employees to sign an NDA.
C. Implement a DLP solution.
D. Use whole disk encryption.

Answer: D

Explanation:
Using whole disk encryption is the best option to protect the data on the remote users’ laptops. Whole disk encryption is a technique that encrypts all data on a hard disk drive, including the operating system, applications and files. Whole disk encryption can prevent unauthorized access to the data if the laptop is lost, stolen or compromised. Whole disk encryption can also protect the data from physical attacks, such as removing the hard disk and connecting it to another device .

NEW QUESTION 221
A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will best accomplish the analyst's objectives?

A. tcpdump -w packetCapture
B. tcpdump -a packetCapture
C. tcpdump -n packetCapture
D. nmap -v > packetCapture
E. nmap -oA > packetCapture

Answer: A

Explanation:
The tcpdump command is a network packet analyzer tool that can capture and display network traffic. The -w option specifies a file name to write the captured packets to, in a binary format that can be read by tcpdump or other tools later. This option is useful for capturing large amounts of network data that will be analyzed at a later time, as the question requires. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called “packetCapture”. The capture must be as efficient as possible, and the -w option minimizes the processing and output overhead of tcpdump, reducing the likelihood that packets will be missed.

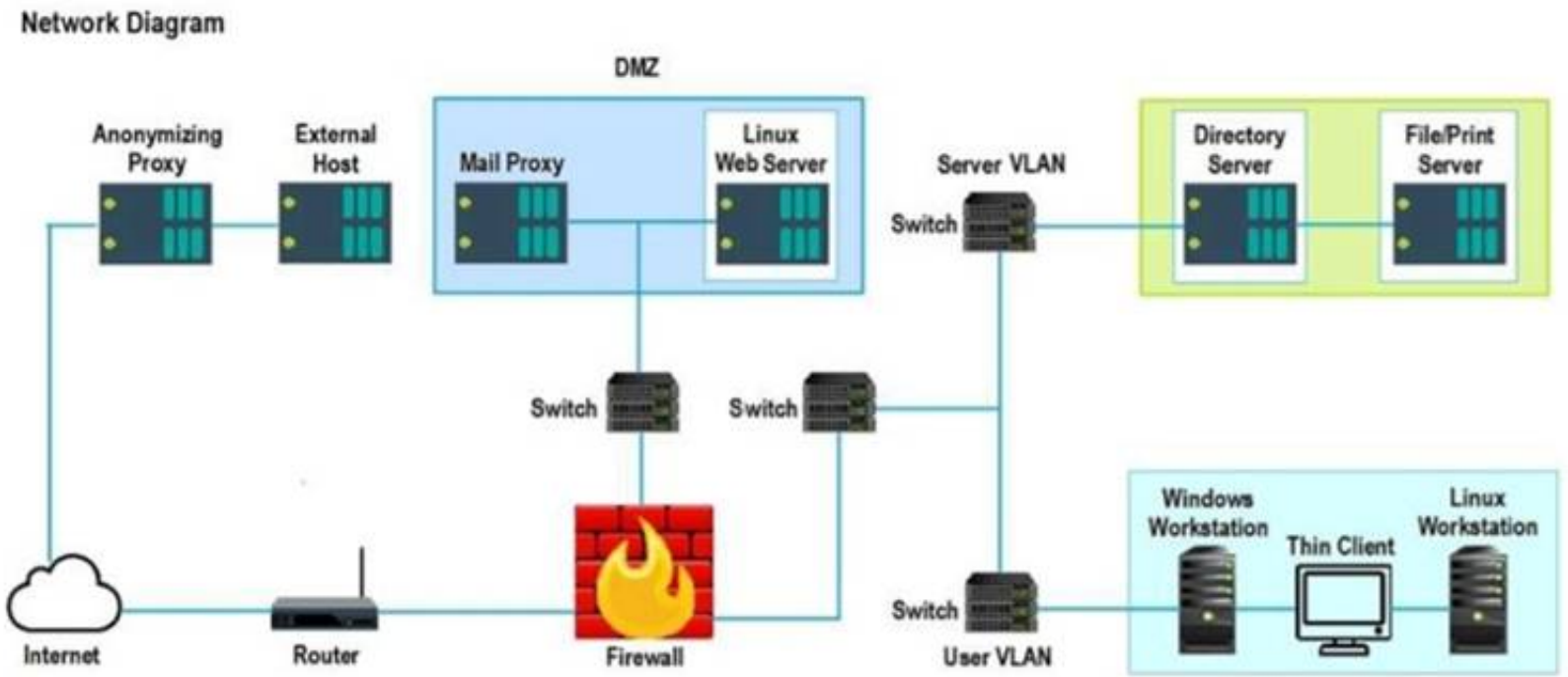
NEW QUESTION 224
A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a Group Policy Object is responsible for the network connectivity Issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?

A. Cl/CD pipeline
B. Impact analysis and reporting
C. Appropriate network segmentation
D. Change management process

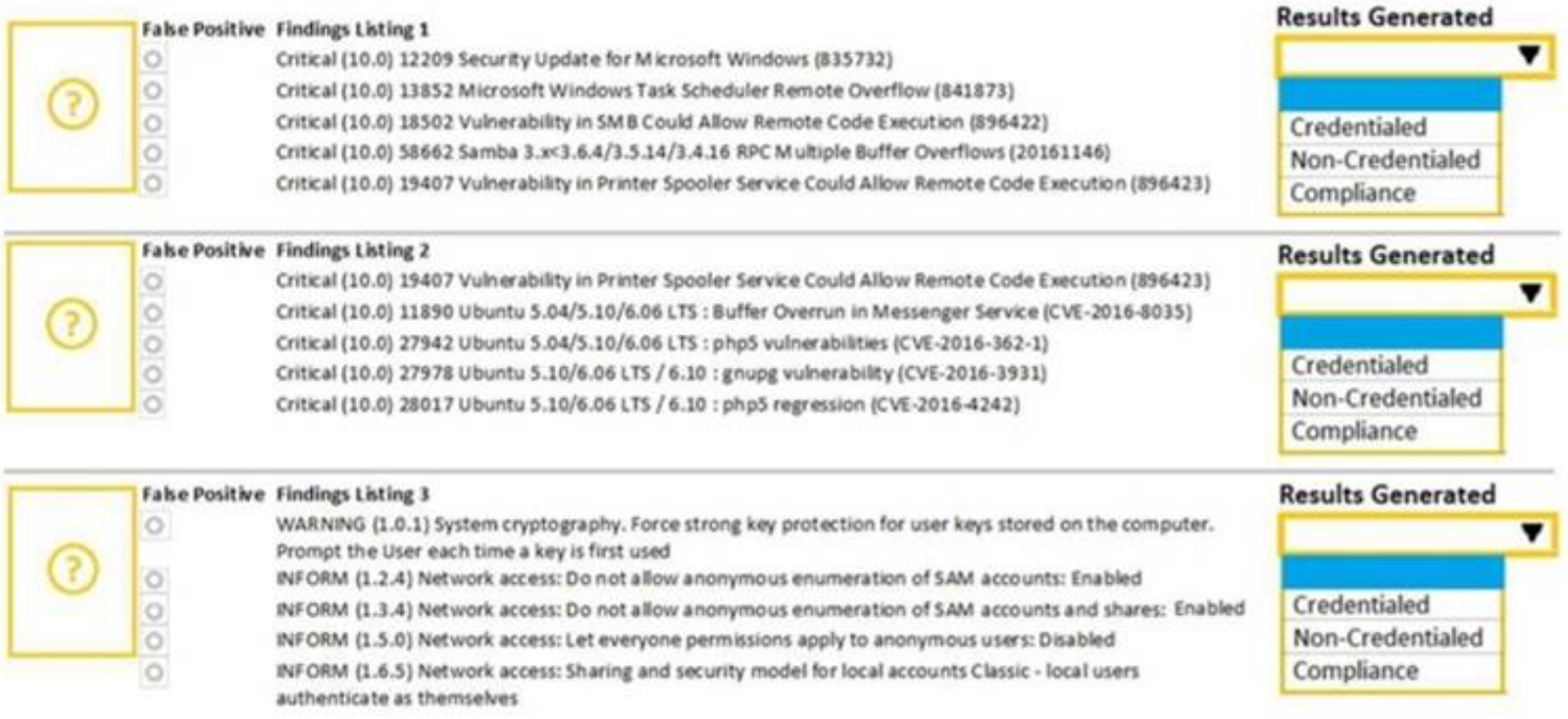
Answer: D

Explanation:
A change management process is a set of procedures that ensures that any changes to a system or service are planned, tested, approved, implemented and documented in a controlled and consistent manner. A change management process can prevent an interruption of service caused by a Group Policy Object (GPO) by ensuring that the GPO is properly configured, tested and authorized before applying it to the servers. A change management process can also provide a way to roll back or undo the changes if they cause any problems.
A CI/CD pipeline is a method of delivering software applications that involves continuous integration (CI) and continuous delivery (CD). CI is the process of merging code changes from multiple developers into a shared repository and testing them automatically. CD is the process of deploying the code changes to different environments (such as testing, staging and production) and releasing them to customers. A CI/CD pipeline does not prevent an interruption of service caused by a GPO, but rather helps to deliver software applications faster and more reliably.
An impact analysis and reporting is a process of assessing the potential effects of a change on a system or service, such as performance, availability, security and compatibility. An impact analysis and reporting can help to identify and mitigate any risks or issues associated with a change. However, an impact analysis and reporting does not prevent an interruption of service caused by a GPO, but rather helps to evaluate and communicate the consequences of a change.
Appropriate network segmentation is a practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, location or security level. Appropriate network segmentation can improve the performance, security and manageability of a network by reducing congestion, isolating threats and controlling access. However, appropriate network segmentation does not prevent an interruption of service caused by a GPO, but rather helps to protect and optimize a network.

NEW QUESTION 225
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Hot Area:

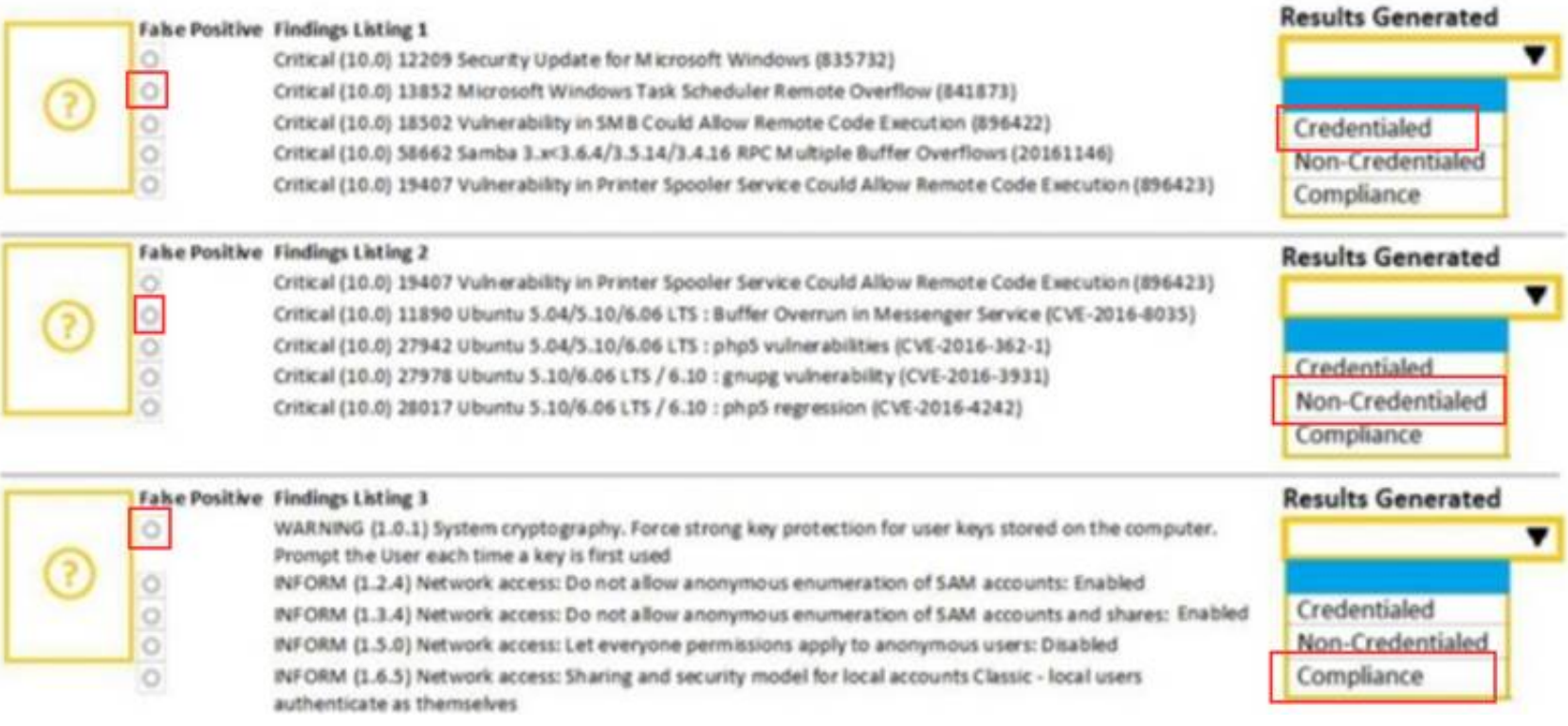


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Hot Area:



NEW QUESTION 227
An analyst is coordinating with the management team and collecting several terabytes of data to analyze using advanced mathematical techniques in order to find patterns and correlations in events and activities. Which of the following describes what the analyst is doing?

A. Data visualization
B. SOAR
C. Machine learning
D. SCAP

Answer: C

Explanation:
The correct answer is C. Machine learning. Machine learning is a branch of artificial intelligence that uses advanced mathematical techniques, such as statistics, algorithms, and linear algebra, to analyze large amounts of data and find patterns and correlations in events and activities. Machine learning can help to automate tasks, improve decision making, and enhance security by detecting anomalies, threats, or trends1.
* A. Data visualization is not correct. Data visualization is the process of presenting data in a graphical or pictorial format, such as charts, graphs, maps, or dashboards. Data visualization can help to communicate information, insights, or trends more effectively and intuitively than using text or numbers alone2.
* B. SOAR is not correct. SOAR stands for Security Orchestration, Automation, and Response, and it is a solution that combines various tools and processes to improve the efficiency and effectiveness of security operations. SOAR can help to automate tasks, integrate systems, coordinate actions, and respond to incidents faster and more consistently3.
* D. SCAP is not correct. SCAP stands for Security Content Automation Protocol, and it is a set of standards and specifications that enable the automated assessment, measurement, and reporting of the security posture of systems and networks. SCAP can help to ensure compliance, identify vulnerabilities, and remediate issues.
* 1: What Is Machine Learning? 2: What Is Data Visualization? 3: What Is Security Orchestration, Auto and Response (SOAR)? : [What Is Security Content Automation Protocol (SCAP)?]

NEW QUESTION 229
A business recently acquired a software company. The software company's security posture is unknown. However, based on an assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?

A. Develop an asset inventory to determine the systems within the software company
B. Review relevant network drawings, diagrams and documentation
C. Perform penetration tests against the software company's Internal and external networks
D. Baseline the software company's network to determine the ports and protocols in use.

Answer: A

Explanation:
An asset inventory is a list of all the hardware, software, data, and other resources that an organization owns or uses. An asset inventory helps to identify what systems are present in an organization, where they are located, what they do, and how they are configured2
Developing an asset inventory is the next step that should be completed to obtain information about the software company’s security posture, as it provides a baseline for further analysis and assessment of the systems’ vulnerabilities and risks.

NEW QUESTION 234
A company uses an FTP server to support its critical business functions The FTP server is configured as follows:
• The FTP service is running with (he data duectory configured in /opt/ftp/data.
• The FTP server hosts employees' home aVectories in /home
• Employees may store sensitive information in their home directories
An loC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C

Explanation:
This would limit the FTP server’s access to a specific directory tree and prevent directory traversal attacks that could access files outside of that tree.
Implementing file-level encryption, supporting FTPS, or upgrading the FTP server would not prevent directory traversal attacks.

NEW QUESTION 239
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

```
1286    ?    Ss    0:00   /usr/sbin/cupsd -f
1287    ?    Ss    0:00   /usr/sbin/httpd
1297    ?    Ssl   0:00   /usr/bin/libvirtd
1301    ?    Ss    0:00   ./usr/sbin/sshd -D
1308    ?    Ss    0:00   /usr/sbin/atd -f
```

Which of the following commands should the administrator run next to further analyze the compromised system?

A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/Is -1 /proc/1301/exe
D. kill -9 1301

Answer: C

Explanation:
/bin/ls -1 /proc/1301/exe is the command that will show the absolute path to the executed binary file associated with the process ID 1301, which is ./usr/sbin/sshd. This information can help the security analyst determine if the binary is an official version and has not been modified, which could be an indicator of a compromise. /proc/1301/exe is a special symbolic link that points to the executable file that was used to start the process 1301 .

NEW QUESTION 240
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations Which of the following would be the BEST method to protect these workstations from threats?

A. Deploy whitelisting to the identified workstations to limit the attack surface
B. Determine the system process centrality and document it
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations

Answer: A

Explanation:
Deploying whitelisting to the identified workstations would be the best method to protect these workstations from threats. Whitelisting is a technique that allows only authorized applications, processes, or users to run or access a system or resource. Whitelisting can help limit the attack surface and prevent malware or unauthorized software from running on a system3. Deploying whitelisting to the workstations that are at the end of life can help mitigate the risk of exploitation due to lack of patches or support from the vendor.

NEW QUESTION 243
An analyst Is reviewing a web developer's workstation for potential compromise. While examining the workstation's hosts file, the analyst observes the following:

```
192.168.3.249    localhost
127.0.0.1        sitedev.local
::1              localhost ip6-localhost ip6-
                 loopback
198.51.100.5     comptia.co
```

Which of the following hosts file entries should the analyst use for further investigation?

A. ::1
B. 127.0.0.1
C. 192.168.3.249
D. 198.51.100.5

Answer: D

Explanation:
The hosts file is a text file that maps hostnames to IP addresses, and it can be used to override DNS resolution. The hosts file entries that should be used for further investigation are the ones that point to external or suspicious IP addresses, such as 198.51.100.5, which is a reserved IP address for documentation purposes. The other entries are either loopback addresses (::1 and 127.0.0.1) or internal network addresses (192.168.3.249), which are less likely to be malicious.

NEW QUESTION 247
At which of the following phases of the SDLC shoukJ security FIRST be involved?

A. Design
B. Maintenance
C. Implementation
D. Analysis
E. Planning
F. Testing

Answer: E

Explanation:
The software development life cycle (SDLC) is a process that consists of several phases that guide the development of software applications or systems. Security should be involved in every phase of the SDLC, but especially in the planning phase, which is the first phase where the scope, objectives, requirements, and resources of the project are defined. By involving security in the planning phase, potential risks and threats can be identified and mitigated early in the process, which can save time, money, and effort later on. Design, maintenance, implementation, analysis, and testing are other phases of the SDLC, but they are not the first phase where security should be involved. Reference:
https://www.bmc.com/blogs/software-development-life-cycle-phases/

NEW QUESTION 248
A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed
C. Review the current blocklist and prioritize it based on the level of threat severit
D. Add the domains with the highest severity to the blocklist.
E. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs

Answer: D

Explanation:
This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION 251
A security analyst is evaluating the following support ticket:
Issue: Marketing campaigns are being filtered by the customer's email servers.
Description: Our marketing partner cannot send emails using our email address. The following log messages were collected from multiple customers:
• The SPF result is PermError.
• The SPF result is SoftFail or Fail.
• The 550 SPF check failed.
Which of the following should the analyst do next?

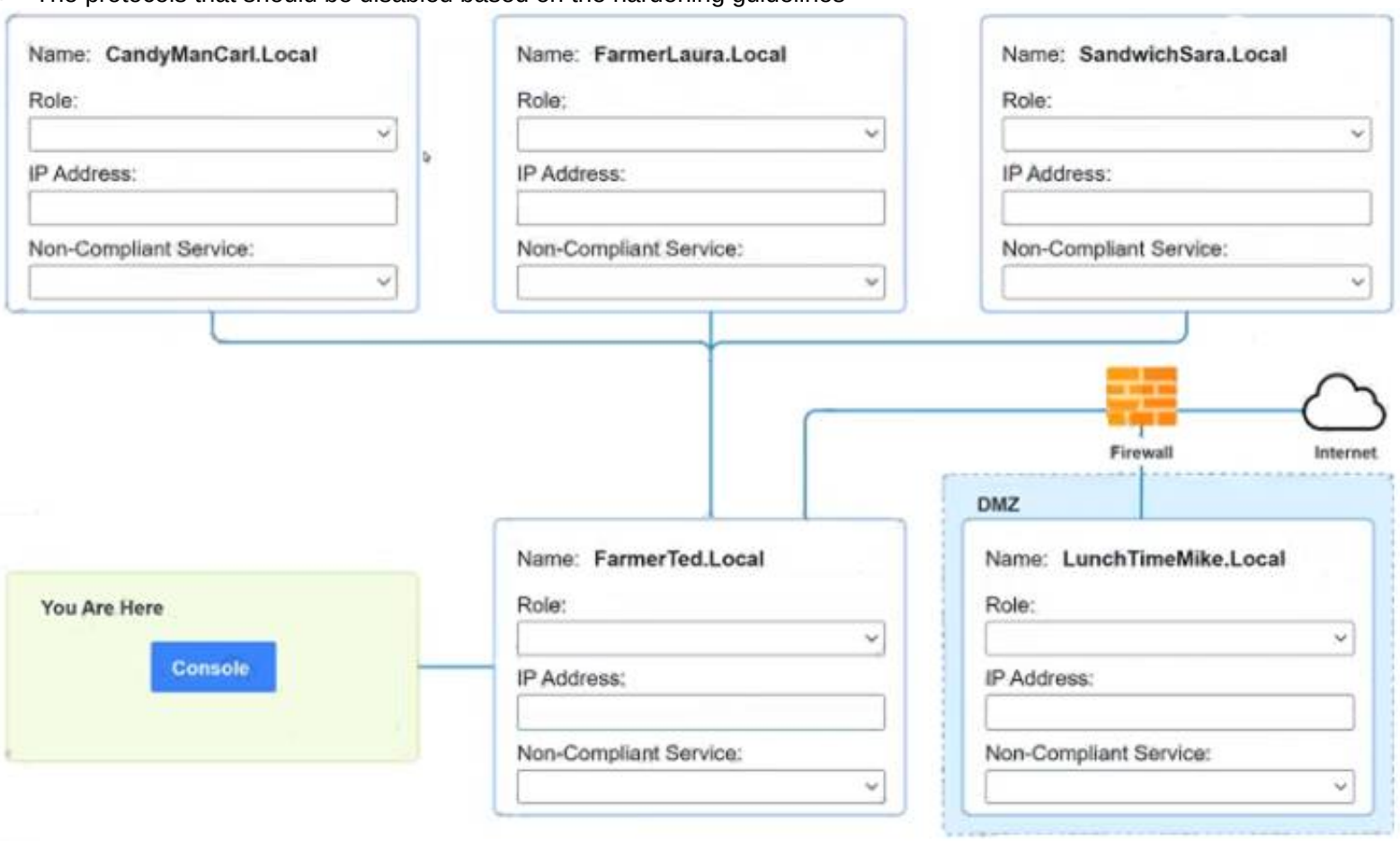
A. Ask the marketing partner's ISP to disable the DKIM setting.
B. Request approval to disable DMARC on the company's ISP.
C. Ask the customers to disable SPF validation.
D. Request a configuration change on the company's public DNS.

Answer: D

Explanation:
The analyst should request a configuration change on the company’s public DNS as the next step, as this can help resolve the issue of marketing campaigns being filtered by the customer’s email servers. The issue is caused by SPF validation failures, which indicate that the marketing partner’s email address is not authorized to send emails on behalf of the company’s domain. SPF stands for Sender Policy Framework, and it is a mechanism that allows domain owners to specify which IP addresses or hosts are allowed to send emails using their domain name. SPF validation is done by checking the SPF record of the sender’s domain in the public DNS, and comparing it with the IP address or host name of the sender’s email server. To fix this issue, the analyst should request a configuration change on the company’s public DNS to add or update the SPF record to include the marketing partner’s email address or IP address as a valid sender.

NEW QUESTION 254
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.

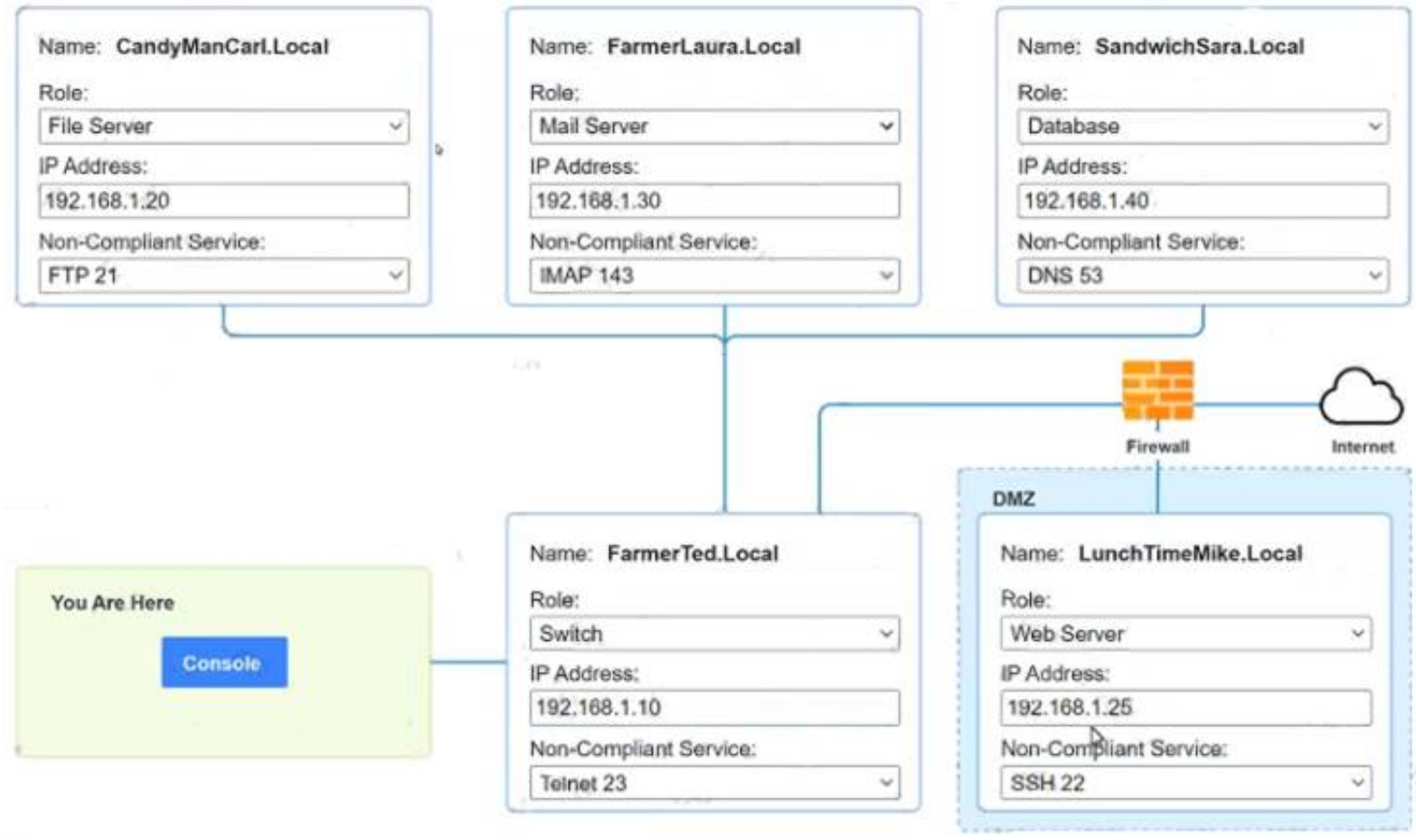
You must determine
- ip address of each device
- The primary server or service each device
- The protocols that should be disabled based on the hardening guidelines

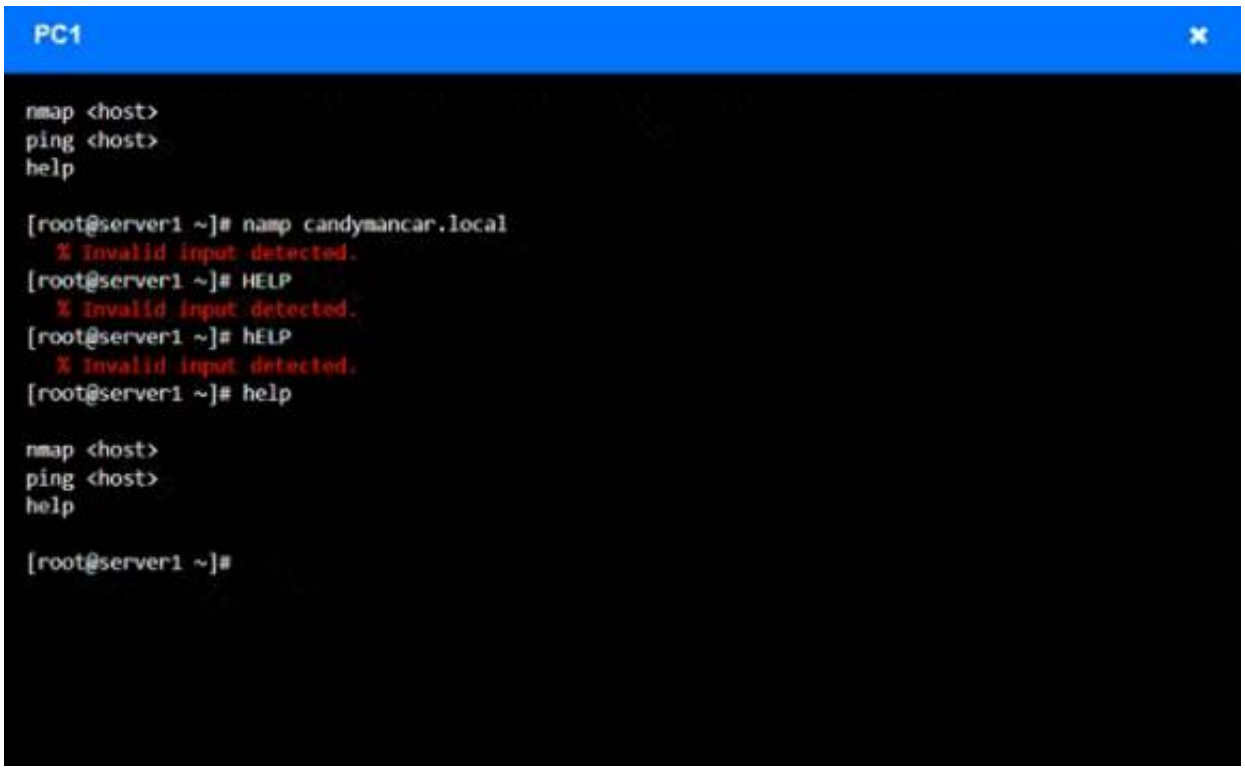


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer below images





NEW QUESTION 259

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

* CS0-002 Practice Questions Verified by Expert Senior Certified Staff

* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year