Practice Exam Questions

CompTIA

CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification

EXAMKILLER

Help Pass Your Exam At First Try

CompTIA

Exam CS0-002

CompTIA CySA+ Certification Exam (CS0-002)

Version: 23.0

[Total Questions: 275]

Question No : 1

An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

A. Change the passwords on the devices.
B. Implement BIOS passwords.
C. Remove the assets from the production network for analysis.
D. Report the findings to the threat intel community.

Answer: C

Explanation: If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.

Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Question No : 2

As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst to coordinate?

A. A black-box penetration testing engagement
B. A tabletop exercise
C. Threat modeling
D. A business impact analysis

Answer: C

Explanation: Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. Reference: https://owasp.org/www-community/Application_Threat_Modeling

Question No : 3

Which of the following is an advantage of SOAR over SIEM?

A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.
C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.

Answer: B

Explanation: SOAR (Security Orchestration, Automation, and Response) reduces the amount of human intervention required, which is an advantage over SIEM (Security Information and Event Management). SIEM is a tool that collects, analyzes, and correlates data from various sources, such as logs, alerts, and events, to provide security monitoring and incident detection. SIEM can help security teams identify and prioritize potential threats, but it still requires manual intervention to investigate and respond to incidents**2**. SOAR is a tool that builds on SIEM by automating and orchestrating various security tasks and workflows, such as incident response, threat hunting, and threat intelligence. SOAR can help security teams reduce manual effort, improve efficiency, and accelerate incident resolution**3**.

Question No : 4

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

A. Implement a mobile device wiping solution for use if a device is lost or stolen.
B. Install a DLP solution to track data now
C. Install an encryption solution on all mobile devices.
D. Train employees to report a lost or stolen laptop to the security department immediately

Answer: A

Explanation: A mobile device wiping solution is a security feature that allows an organization to remotely erase or delete all data on a mobile device if it is lost or stolen**2** A mobile device wiping solution can help protect the privacy of the data on a device and prevent unauthorized access or disclosure of sensitive information. A mobile device wiping solution can be implemented using built-in features of some mobile operating systems, third-party applications, or mobile device management (MDM) software.
Reference: **2** What Is Mobile Device Wiping? | Shred-it UK

Question No : 5

Which of the following are considered PII by themselves? (Select TWO).

A. Government ID
B. Job title
C. Employment start date
D. Birth certificate
E. Employer address
F. Mother's maiden name

Answer: A,D

Explanation: PII (Personally Identifiable Information) is any information that can be used to identify, contact, or locate a specific individual, either by itself or when combined with other information**1**. PII by itself is information that can uniquely identify an individual without any additional information. Examples of PII by itself are:

- Government ID. A government ID is a number or code that is issued by a government authority to an individual for identification purposes. Examples of government IDs are social security numbers, passport numbers, driver's license numbers, etc. A government ID can uniquely identify an individual without any additional information.

- Birth certificate. A birth certificate is a document that records the birth of an individual and contains information such as name, date of birth, place of birth, parents' names, etc. A birth certificate can uniquely identify an individual without any additional information.

Other examples of PII by itself are biometric data, DNA profile, fingerprints, etc. Examples of information that are not PII by themselves are:

- Job title. A job title is a name or description of a position or role in an organization. A job title does not uniquely identify an individual without any additional information, as many individuals can have the same job title.
- Employment start date. An employment start date is the date when an individual began working for an organization. An employment start date does not uniquely identify an individual without any additional information, as many individuals can have the same employment start date.
- Employer address. An employer address is the location of an organization where an individual works. An employer address does not uniquely identify an individual without any additional information, as many individuals can work at the same employer address.
- Mother's maiden name. A mother's maiden name is the surname that a woman had before she married. A mother's maiden name does not uniquely identify an individual without any additional information, as many individuals can have the same mother's maiden name.

Other examples of information that are not PII by themselves are gender, race, ethnicity, age, etc.

Reference: **1**: https://www.techopedia.com/definition/23889/personally-identifiable-information-pii

Question No : 6 CORRECT TEXT

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

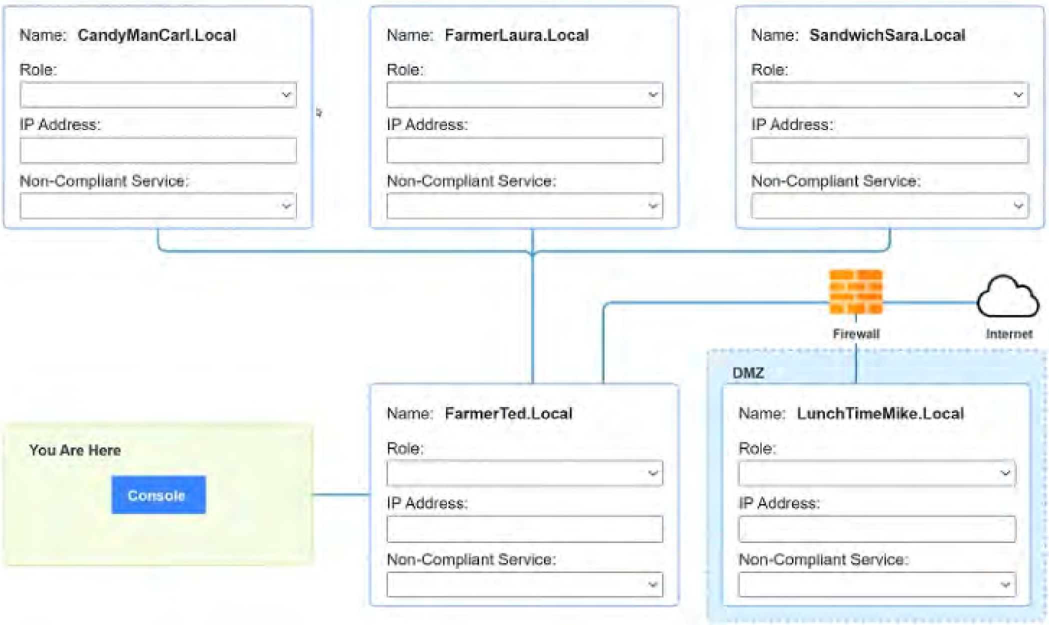
Instructions :

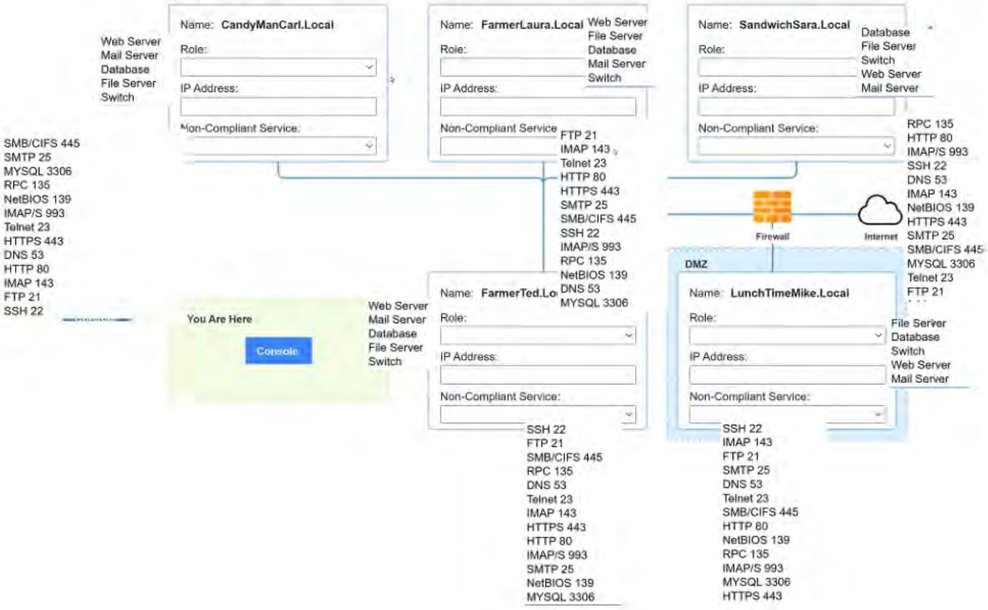
- Using the available tools, discover devices on the corporate network and the services running on these devices.

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

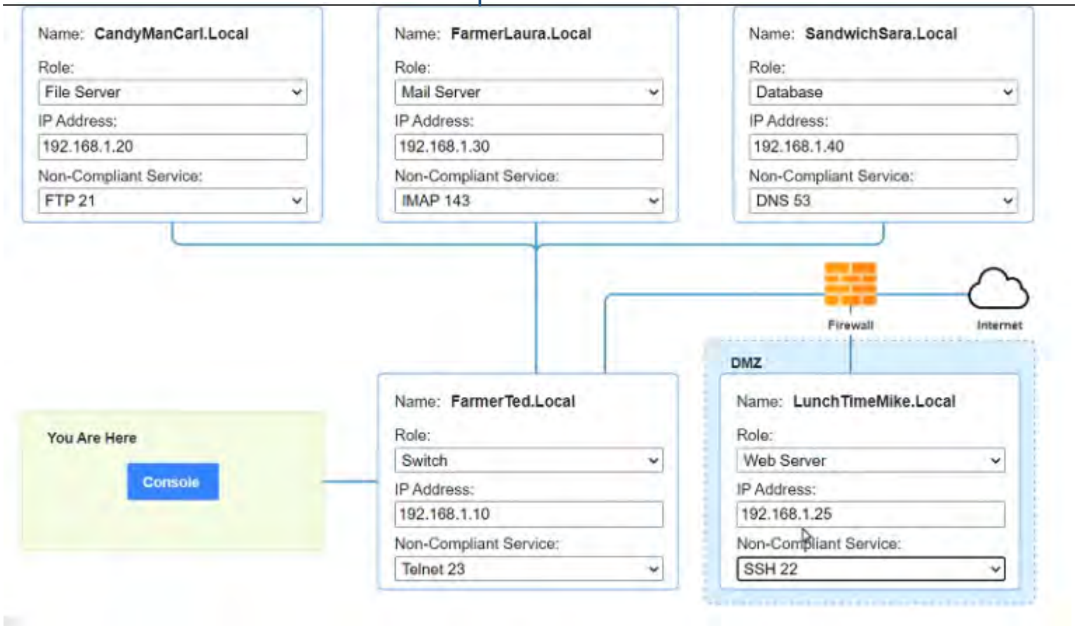




Answer: see the answer below in explanation:

Explanation:

Answer below images



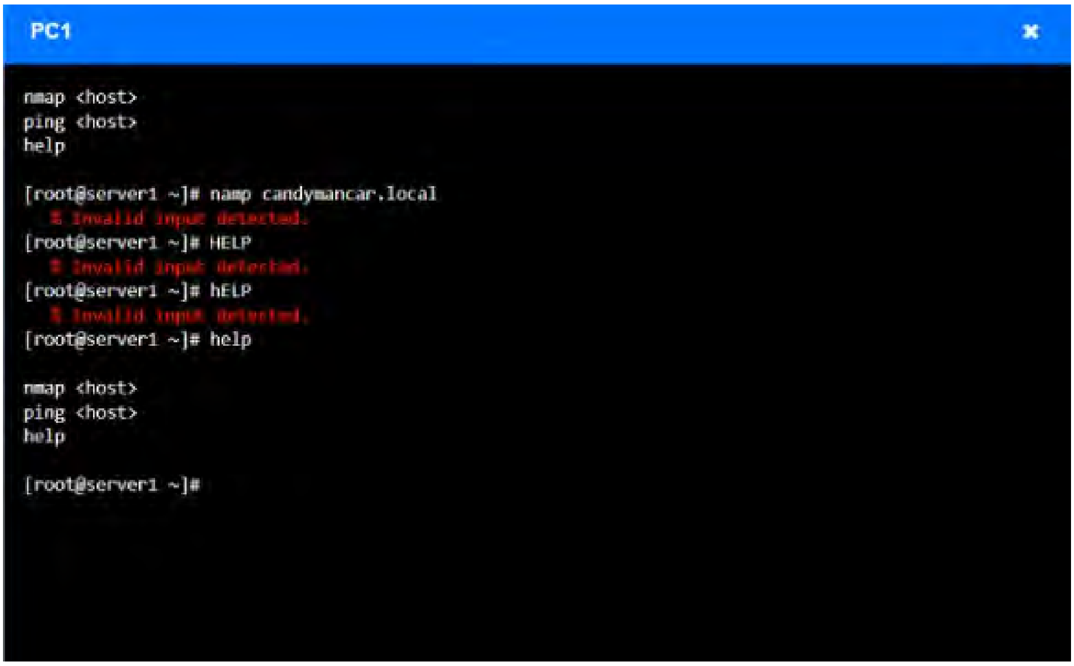
Name: CandyManCarl.Local
Role: File Server
IP Address: 192.168.1.20
Non-Compliant Service: FTP 21

Name: FarmerLaura.Local
Role: Mail Server
IP Address: 192.168.1.30
Non-Compliant Service: IMAP 143

Name: SandwichSara.Local
Role: Database
IP Address: 192.168.1.40
Non-Compliant Service: DNS 53

Name: FarmerTed.Local
Role: Switch
IP Address: 192.168.1.10
Non-Compliant Service: Telnet 23

Name: LunchTimeMike.Local
Role: Web Server
IP Address: 192.168.1.25
Non-Compliant Service: SSH 22



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

[root@server1 ~]# namp candymancar.local
   % Invalid input detected.
[root@server1 ~]# HELP
   % Invalid input detected.
[root@server1 ~]# hELP
   % Invalid input detected.
[root@server1 ~]# help

nmap <host>
ping <host>
help

[root@server1 ~]#
```

Question No : 7

A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.

Answer: C

Explanation: The security team should perform postmortem data correlation next after receiving notification of the incident from the help desk technician. Postmortem data correlation is an activity that involves analyzing data from various sources (such as logs, alerts, reports, etc.) to identify root causes, impacts, indicators of compromise (IoCs), lessons learned, and recommendations for improvement after an incident**3**. Postmortem data correlation can help the security team to:

- Determine how the incident occurred and how it was detected and resolved
- Assess the scope and severity of the incident and its effects on confidentiality, integrity, and availability
- Identify any gaps or weaknesses in security controls or processes that contributed to the incident
- Develop action plans or remediation strategies to prevent recurrence or mitigate future incidents

Question No : 8

Which of the following is the BEST way to gather patch information on a specific server?

A. Event Viewer
B. Custom script
C. SCAP software
D. CI/CD

Answer: B

Explanation: A custom script is a piece of code that can be written to perform a specific task or automate a process. A custom script can be used to gather patch information on a specific server by querying the server's operating system, registry, or patch management software and retrieving the relevant data. A custom script can be more flexible and efficient than other methods, such as Event Viewer, SCAP software, or CI/CD, which may not provide the exact information needed or may require additional steps or tools.

Question No : 9

A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

A. The whitelist
B. The DNS
C. The blocklist
D. The IDS signature

Answer: D

Explanation: The IDS signature should be updated next after receiving a new IoC (Indicator of Compromise) from an ISAC (Information Sharing and Analysis Center) that follows a threat actor's profile and activities. An IoC is a piece of evidence or artifact that suggests a system or network has been compromised or attacked by a threat actor**4**. An IoC can be an IP address, domain name, URL, file hash, email address, registry key, etc. An ISAC is a nonprofit organization that collects, analyzes, and shares threat intelligence and best practices among its members within a specific sector or industry**5**. An ISAC can help to improve the security awareness and preparedness of its members by providing timely and relevant information about emerging threats and incidents.

Question No : 10

Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

A. To establish a clear chain of command
B. To meet regulatory requirements for timely reporting
C. To limit reputation damage caused by the breach
D. To remediate vulnerabilities that led to the breach
E. To isolate potential insider threats
F. To provide secure network design changes

Answer: B,C

Explanation: Reporting processes are important to include when updating an incident response plan after a breach for several reasons. Two of the most likely reasons are:

- To meet regulatory requirements for timely reporting. Many regulations and standards require organizations to report security incidents or breaches within a certain time frame or face penalties or sanctions. For example, the General Data Protection Regulation (GDPR) requires organizations to report personal data breaches within 72 hours of becoming aware of them. Reporting processes can help organizations to comply with these requirements by defining who, what, when, where, how, and why to report incidents or breaches.
- To limit reputation damage caused by the breach. Security incidents or breaches can have negative impacts on an organization's reputation, trust, and customer

loyalty. Reporting processes can help organizations to limit these impacts by communicating effectively and transparently with internal and external stakeholders, such as employees, customers, partners, regulators, media, and public. Reporting processes can help organizations to provide accurate and consistent information about the breach, its causes, impacts, and remediation actions.

Other possible reasons to include reporting processes when updating an incident response plan after a breach are:

- To establish a clear chain of command (A). Reporting processes can help organizations to establish a clear chain of command for incident response by defining roles and responsibilities, escalation procedures, and decision-making authority.
- To remediate vulnerabilities that led to the breach (D). Reporting processes can help organizations to remediate vulnerabilities that led to the breach by documenting and analyzing the root causes, lessons learned, and best practices for improvement.
- To isolate potential insider threats (E). Reporting processes can help organizations to isolate potential insider threats by monitoring and auditing user activities, behaviors, and access rights before, during, and after the breach.

References: : https://gdpr.eu/data-breach-notification/ :
https://www.techopedia.com/definition/13493/penetration-testing :
https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

Question No : 11

While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped

Answer: C,F

Explanation: The most secure states for the certificate authority server when it is not in use are powered off and air gapped. Powering off the server will prevent any unauthorized access or tampering with the server while it is idle. Air gapping the server will isolate it from any network connections, making it inaccessible to remote attackers or malware. These measures will help to protect the integrity and confidentiality of the certificate authority server and its keys.

Question No : 12

A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited

resources to support testing. Which of the following exercises would be the best approach?

A. Tabletop scenarios
B. Capture the flag
C. Red team vs. blue team
D. Unknown-environment penetration test

Answer: A

Explanation: A tabletop scenario is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. A tabletop scenario is the best approach for a company that wants to test a new incident response plan without impacting the environment or using many resources. A tabletop scenario can help the company identify strengths and weaknesses in their plan, clarify roles and responsibilities, and improve communication and coordination among team members. The other options are more intensive and disruptive exercises that involve simulating a real incident or attack. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.linkedin.com/pulse/tabletop-exercises-explained-matt-lemon-phd

Question No : 13

A user reports a malware alert to the help desk. A technician verities the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do next?

A. Document the procedures and walk through the incident training guide.
B. Reverse engineer the malware to determine its purpose and risk to the organization.
C. Sanitize the workstation and verify countermeasures are restored.
D. Isolate the workstation and issue a new computer to the user.

Answer: C

Explanation: Sanitizing the workstation and verifying countermeasures are restored are part of the eradication and recovery processes that the security analyst should perform next. Eradication is the process of removing malware or other threats from the affected systems, while recovery is the process of restoring normal operations and functionality to the affected systems. Sanitizing the workstation can involve deleting or wiping any malicious files or programs, while verifying countermeasures are restored can involve checking and updating any security controls or settings that may have been compromised . Reference: https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/

Question No : 14

A forensic analyst is conducting an investigation on a compromised server Which of the following should the analyst do first to preserve evidence''

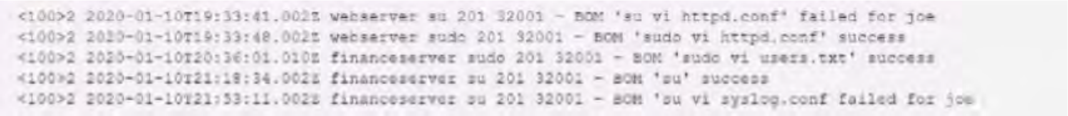
A. Restore damaged data from the backup media
B. Create a system timeline
C. Monitor user access to compromised systems
D. Back up all log files and audit trails

Answer: D

Explanation: A forensic analyst is conducting an investigation on a compromised server. The first step that the analyst should do to preserve evidence is to back up all log files and audit trails. This will ensure that the analyst has a copy of the original data that can be used for analysis and verification. Backing up the log files and audit trails will also prevent any tampering or modification of the evidence by the attacker or other parties. The other options are not the first steps or may alter or destroy the evidence. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

Question No : 15

An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:



```
<100>2 2020-01-10T19:33:41.002Z webserver su 201 32001 - BOM 'su vi httpd.conf' failed for joe
<100>2 2020-01-10T19:33:48.002Z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' success
<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002Z financeserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

Which of the following entries should cause the analyst the MOST concern?

A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
B. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
D. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success

Answer: D

Explanation: The syslog entries show the attempts of users to run commands with elevated permissions on two servers: webserver and financeserver. The entries include the date and time, the server name, the command used (su or sudo), the user name, and the outcome (success or failed). The policy of the organization states that users should always run commands under their own account, with temporary administrator privileges if necessary. This means that users should use sudo to run commands as another user (usually root), rather than su to switch to another user's account. Therefore, the entry that should cause the analyst the most concern is D. <100> 2020-01-10T19:34…002z financeserver su 201 32001 = BOM ' su vi success. This entry shows that someone used su to switch to another user's account on the financeserver and successfully edited a file with vi. This could indicate an unauthorized access or a compromised account.
Reference: What is the difference between "su" and "sudo"? | Ask Ubuntu

Question No : 16

A security analyst is attempting to resolve an incident in which highly confidential company pricing information was sent to clients. It appears this information was unintentionally sent by an employee who attached it to public marketing material. Which of the following configuration changes would work BEST to limit the risk of this incident being repeated?

A. Add client addresses to the blocklist.
B. Update the DLP rules and metadata.
C. Sanitize the marketing material.

D. Update the insider threat procedures.

Answer: B

Explanation: Data Loss Prevention (DLP) is a security technology designed to detect, prevent, and respond to the unauthorized disclosure of confidential data. By updating the DLP rules and metadata, it is possible to better define what types of confidential information can be shared and limit access to any sensitive documents.

DLP rules and metadata can help to identify, classify and label sensitive data based on its content and context. DLP rules and metadata can also help to enforce actions or policies on sensitive data, such as blocking, encrypting or alerting .
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

Question No : 17

After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

Answer: B

Explanation: File carving is a technique that involves scanning the raw data bytes of a hard disk and rebuilding files by using information found in file headers and footers. File carving can help recover files that have been deleted or corrupted or that are not recognized by the file system. File carving does not rely on metadata or directory structures to locate files, but rather on file signatures or patterns that indicate the start and end of files. File carving can be performed manually or automatically using tools or software that support various file formats. Header analysis (A) is a technique that involves examining file headers to determine file types or formats. Header analysis can help identify files that have been renamed or disguised or that have unknown extensions. Header analysis does not involve reconstructing files by scanning raw data bytes. Metadata analysis © is a technique that involves examining metadata to extract information about files or file systems. Metadata analysis can help determine file attributes such as name, size, date, location, owner, etc. Metadata analysis does not involve reconstructing files by scanning raw data bytes

Question No : 18

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 provider**1**. 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 data**2**. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

Question No : 19

An organization wants to consolidate a number of security technologies throughout the organization and standardize a workflow for identifying security issues prioritizing the severity and automating a response Which of the following would best meet the organization's needs'?

A. MaaS
B. SIEM
C. SOAR
D. CI/CD

Answer: C

Explanation: A security orchestration, automation, and response (SOAR) system is a solution that combines various security technologies and workflows to identify security issues, prioritize their severity, and automate a response. A SOAR system can help an organization consolidate its security tools and processes and standardize its workflow for incident response. The other options are not relevant or comprehensive for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-and-response-soar

Question No : 20

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 rules **3**. DLP can also track and classify data assets based on various criteria, such as name, type, content, or data profile**4**. DLP can help protect data from insider threats, external attackers, or human errors.

Question No : 21

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

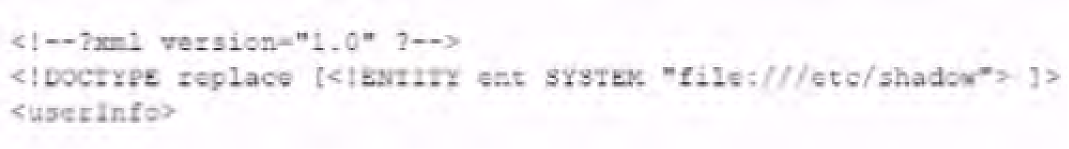
B. Searching
C. Clustering
D. Grouping

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.

Question No : 22

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:



```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following it the BEST solution to mitigate this type of attack?

A. Implement a better level of user input filters and content sanitization.
B. Property configure XML handlers so they do not process sent parameters coming from user inputs.
C. Use parameterized Queries to avoid user inputs horn being processed by the server.
D. Escape user inputs using character encoding conjoined with whitelisting

Answer: A

Explanation: The piece of code in the XML file is an example of a command injection attack, which is a type of attack that exploits insufficient input validation or output encoding to execute arbitrary commands on a server or system**2** The attacker can inject malicious commands into an XML element that is processed by an XML handler on the server, and cause the server to execute those commands. The best solution to mitigate this type of attack is to implement a better level of user input filters and content sanitization, which means checking and validating any user input before processing it, and removing or encoding any potentially harmful characters or commands.
Reference: **2** Command Injection - OWASP

Question No : 23

While observing several host machines, a security analyst notices a program is overwriting data to a buffer. Which of the following controls will best mitigate this issue?

A. Data execution prevention
B. Output encoding
C. Prepared statements
D. Parameterized queries

Answer: A

Explanation: Data execution prevention (DEP) is a security feature that prevents code from being executed in memory regions that are marked as data-only. This helps mitigate buffer overflow attacks, which are a type of attack where a program overwrites data to a buffer beyond its allocated size, potentially allowing malicious code to be executed. DEP can be implemented at the hardware or software level and can prevent unauthorized code execution in memory buffers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention

Question No : 24

A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption
B. eFuse
C. Secure Enclave
D. Trusted execution

Answer: B

Explanation: An eFuse, or electronic fuse, is a microscopic fuse put into a computer chip that can be blown by applying a high voltage or current. Once blown, an eFuse cannot be reset or repaired, and its state can be read by software or hardware**2** An eFuse can be used by a hardware manufacturer to prevent firmware downgrades on a system-on-chip (SoC) that will be used by mobile devices. An eFuse can store information such as the

firmware version, security level, or device configuration on the chip. When a newer firmware is installed, an eFuse can be blown to indicate the update and prevent reverting to an older firmware. This can help protect the device from security vulnerabilities, compatibility issues, or unauthorized modifications.
Reference: **2** eFuse - Wikipedia

Question No : 25

An organization has the following policies:

*Services must run on standard ports.

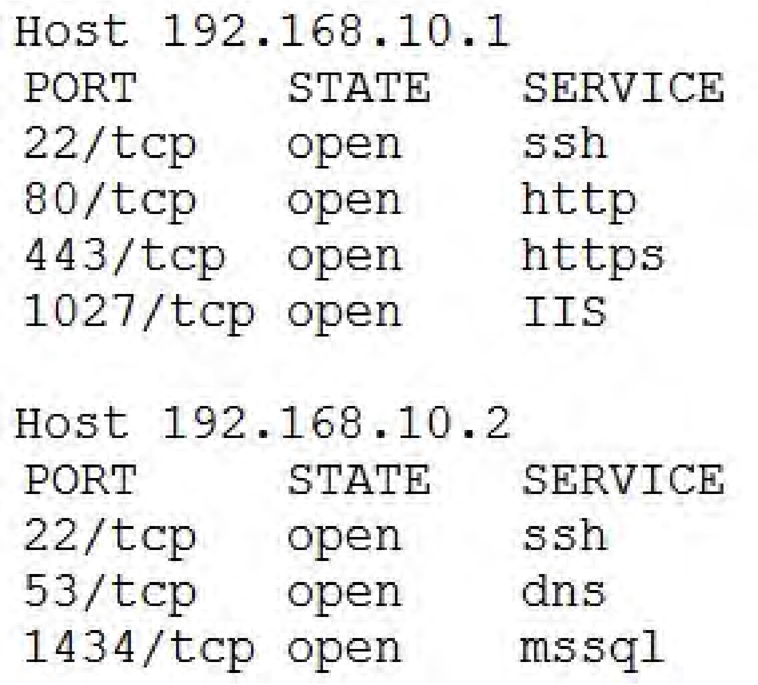
*Unneeded services must be disabled.

The organization has the following servers:

*192.168.10.1 - web server

*192.168.10.2 - database server

A security analyst runs a scan on the servers and sees the following output:



```
Host 192.168.10.1
 PORT      STATE   SERVICE
 22/tcp    open    ssh
 80/tcp    open    http
 443/tcp   open    https
 1027/tcp  open    IIS

Host 192.168.10.2
 PORT      STATE   SERVICE
 22/tcp    open    ssh
 53/tcp    open    dns
 1434/tcp  open    mssql
```

Which of the following actions should the analyst take?

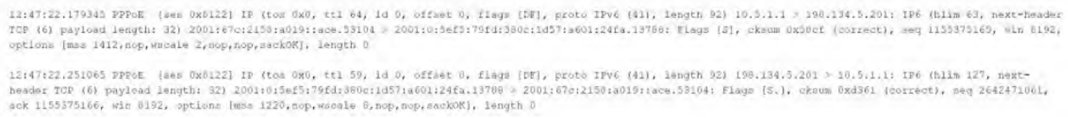
A. Disable HTTPS on 192.168.10.1.
B. Disable IIS on 192.168.10.1.
C. Disable DNS on 192.168.10.2.
D. Disable MSSQL on 192.168.10.2.
E. Disable SSH on both servers.

Answer: E

Explanation: SSH stands for Secure Shell, which is a protocol that allows remote access and administration of a server. If the organization has a policy that services must run on standard ports and unneeded services must be disabled, then SSH should be disabled on both servers, because it runs on port 22, which is not a standard port for a web server or a database server, and it is not needed for those servers to function properly. Disabling HTTPS on 192.168.10.1, disabling IIS on 192.168.10.1, disabling DNS on 192.168.10.1, or disabling MSSQL on 192.168.10.2 are not appropriate actions, because they would affect the functionality of the web server or the database server and violate the organization's policy of running services on standard ports. Reference: https://www.ssh.com/ssh/port

Question No : 26

The following output is from a tcpdump al the edge of the corporate network:



```
12:47:22.179345 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 10.5.1.1 > 198.134.5.201: IP6 (hlim 63, next-header
TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788: Flags [S], cksum 0x58cf (correct), seq 1155375165, win 8192,
options [mss 1412,nop,wscale 2,nop,nop,sackOK], length 0

12:47:22.251065 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 198.134.5.201 > 10.5.1.1: IP6 (hlim 127, next-
header TCP (6) payload length: 32) 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788 > 2001:67c:2158:a019::ace.53104: Flags [S.], cksum 0xd361 (correct), seq 2642471061,
ack 1155375166, win 8192, options [mss 1220,nop,wscale 0,nop,nop,sackOK], length 0
```

Which of the following best describes the potential security concern?

A. Payload lengths may be used to overflow buffers enabling code execution.
B. Encapsulated traffic may evade security monitoring and defenses
C. This traffic exhibits a reconnaissance technique to create network footprints.
D. The content of the traffic payload may permit VLAN hopping.

Answer: B

Explanation: Encapsulated traffic may evade security monitoring and defenses by hiding or obfuscating the actual content or source of the traffic. Encapsulation is a technique that wraps data packets with additional headers or protocols to enable communication across different network types or layers. Encapsulation can be used for legitimate purposes, such as tunneling, VPNs, or NAT, but it can also be used by attackers to bypass security controls or detection mechanisms that are not able to inspect or analyze the encapsulated traffic .
Reference: https://www.techopedia.com/definition/10339/memory-dump

Question No : 27

Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

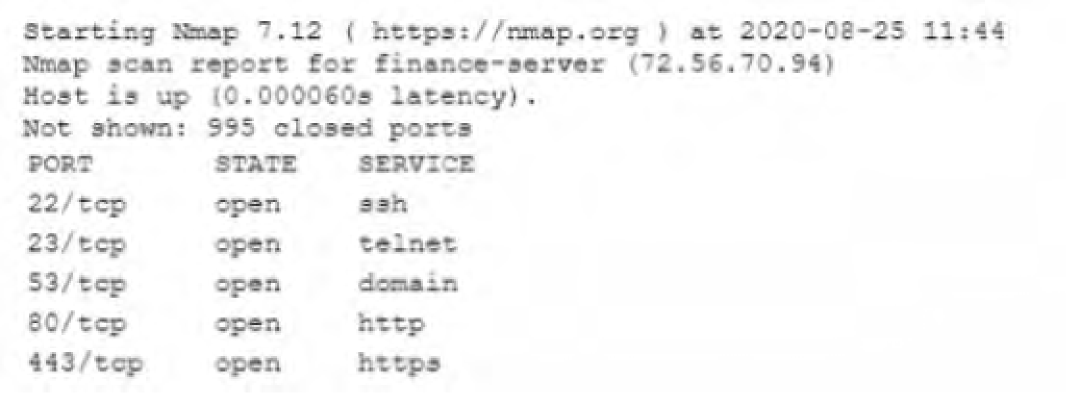
A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

Answer: B

Explanation: The disclosure section of an organization’s incident response plan should cover how the organization handles public or private disclosures of an incident. The disclosure section should contain the organization’s legal and regulatory requirements regarding disclosures, such as the type, content, format, timing, and recipients of the disclosures. The disclosure section should also specify the roles and responsibilities of the personnel involved in the disclosure process, such as who is authorized to make or approve disclosures, who is responsible for communicating with internal and external stakeholders, and who is accountable for ensuring compliance with the disclosure requirements. The disclosure section should not focus on how to reduce the likelihood customers will leave due to the incident (A), as this is a business objective rather than a disclosure requirement. The disclosure section should not include the names and contact information of key employees who are needed for incident resolution ©, as this is an operational detail rather than a disclosure requirement. The disclosure section should not contain language explaining how the organization will reduce the likelihood of the incident from happening in the future (D), as this is a remediation action rather than a disclosure requirement.
Reference: https://www.techopedia.com/definition/24771/technical-controls

Question No : 28

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

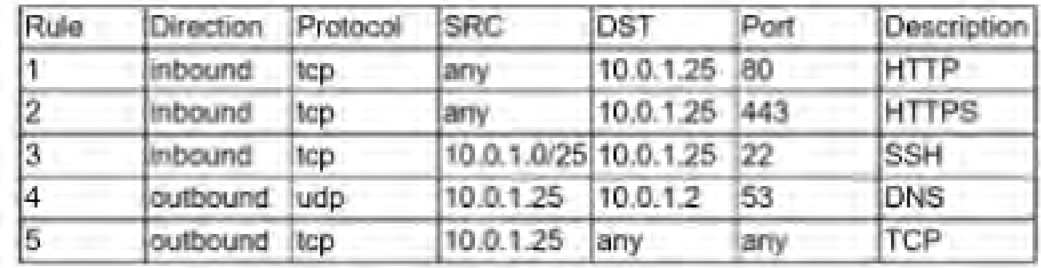
Answer: D,F

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

Question No : 29

A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.

The network rules for the instance are the following:



Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?

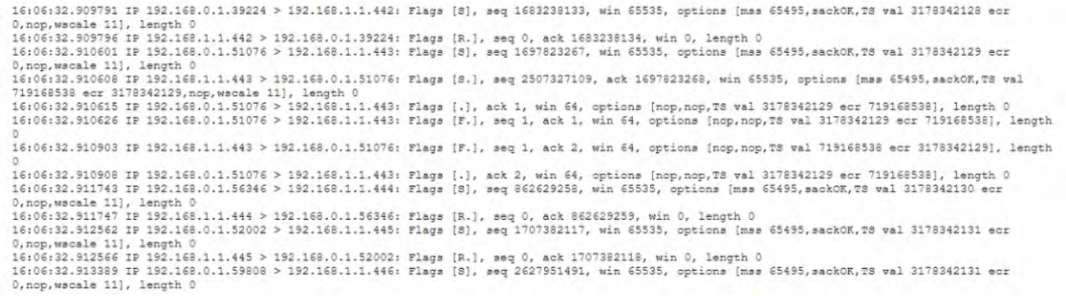
A. Remove rules 1.2. and 3.
B. Remove rules 1.2. 4. and 5.
C. Remove rules 1.2. 3.4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.4. and 5.
F. Remove rules 4 and 5

Answer: C

Explanation: The best way to isolate and triage the host is to remove rules 1, 2, 3, 4, and 5. These rules allow inbound and outbound traffic on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) from any source or destination. By removing these rules, the security analyst can block any network communication to or from the host, preventing any further data exfiltration or malware infection. This will also allow the security analyst to perform a forensic analysis on the host without any interference from external sources.

Question No : 30

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 192.168.0.1.59808 > 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.

Question No : 31

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

A. Automate the use of a hashing algorithm after verified users make changes to their data.
B. Use encryption first and then hash the data at regular, defined times.
C. Use a DLP product to monitor the data sets for unauthorized edits and changes.
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: A

Explanation: Automating the use of a hashing algorithm after verified users make changes to their data is an appropriate course of action to verify that a user’s data is not altered without the user’s consent. Hashing is a technique that produces a unique and fixed-length value for a given input, such as a file or a message. Hashing can help to verify the data integrity by comparing the hash values of the original and modified data. If the hash values match, then the data has not been altered without the user’s consent. If the hash values differ, then the data may have been tampered with or corrupted .

Question No : 32

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?