CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
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 2
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

A. Fully segregate the affected servers physically in a network segment, apart from the production network.
B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
D. Collect all the files that have changed and compare them with the previous baseline

Answer: C

Explanation:
The first action that should be taken to prevent a more serious compromise is to check the hash signatures, comparing them with malware databases to verify if the files are infected. This will help to determine if the changes to hash signatures were caused by malicious software or legitimate updates. If the files are infected, they should be quarantined and removed from the network. Checking the hash signatures will also help to identify the type and source of the malware, which can inform further actions such as blocking malicious domains or IPs, updating antivirus signatures, or notifying users3.

NEW QUESTION 3
A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:

A. a tabletop exercise
B. a business impact analysis
C. a PCI assessment
D. an application stress test.

Answer: C

Explanation:
A PCI assessment should be conducted prior to the deployment of a new application that contains SPI (Sensitive Personal Information). A PCI assessment is an evaluation of how well an organization complies with the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements for protecting cardholder data. PCI DSS applies to any organization that stores, processes, or transmits cardholder data, such as credit card numbers, expiration dates, or security codes4. A PCI assessment can help identify and remediate any gaps or weaknesses in the security controls of an application that handles cardholder data.

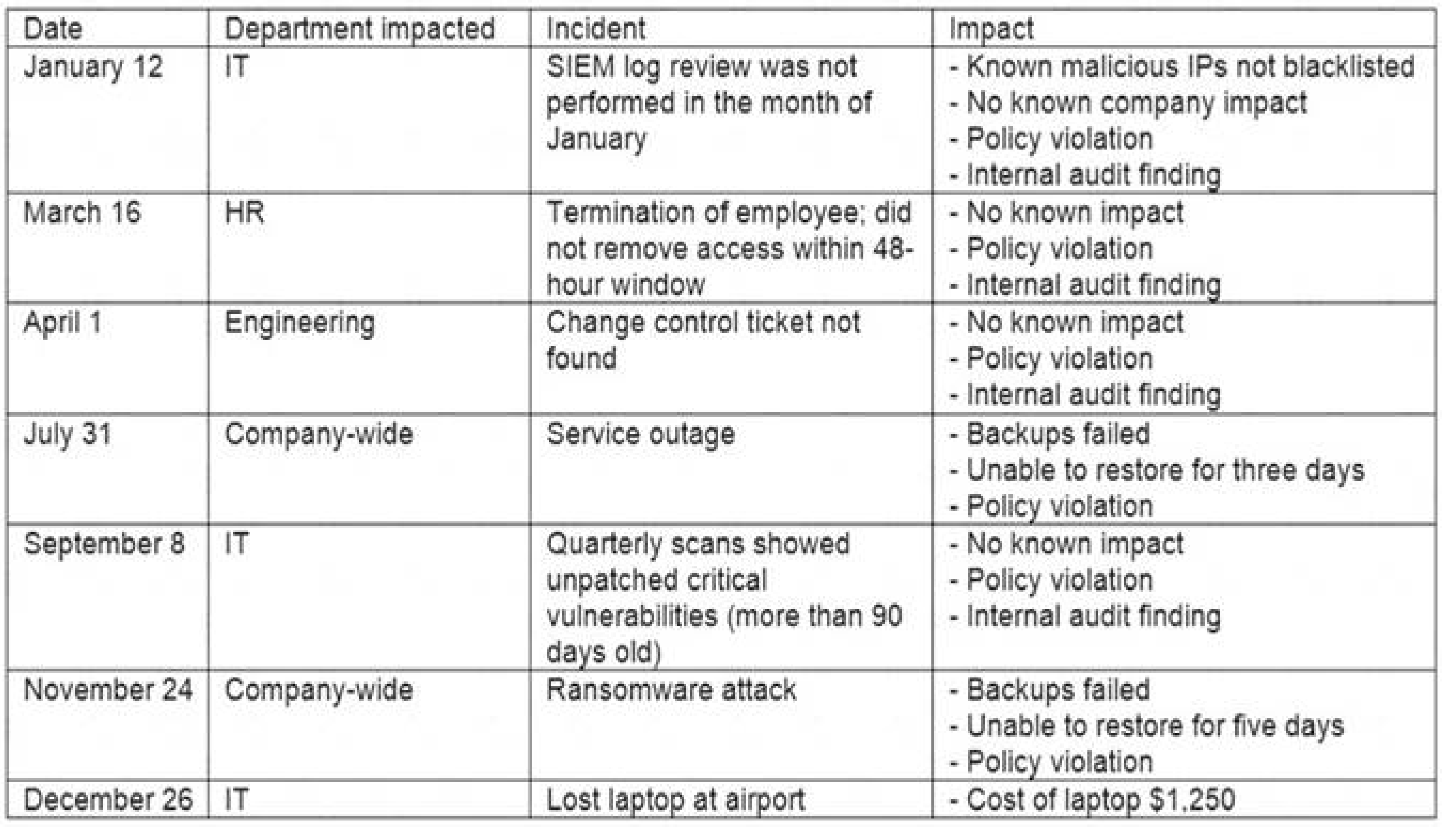
NEW QUESTION 4
An organization wants to collect loCs from multiple geographic regions so it can sell the information to its customers. Which of the following should the organization deploy to accomplish this task?

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 5
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year. Below is the incident register for the organization:



Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

Which of the following should the organization consider investing in first due to the potential impact of availability?

A. Hire a managed service provider to help with vulnerability management.
B. Build a warm site in case of system outages.
C. Invest in a failover and redundant system, as necessary.
D. Hire additional staff for the IT department to assist with vulnerability management and log review.

Answer: C

Explanation:
Investing in a failover and redundant system, as necessary, is the best solution to improve the availability of the organization's systems based on past incidents. A failover system is a backup system that automatically takes over the operation of a primary system in case of a failure or outage. A redundant system is a duplicate system that runs simultaneously with the primary system and provides backup functionality if needed. Investing in a failover and redundant system can help to ensure that the organization's systems are always available and can handle the workload without interruption or degradation .

NEW QUESTION 6
An application has been updated to fix a vulnerability. Which of the following would ensure that previously patched vulnerabilities have not been reintroduced?

A. Stress testing
B. Regression testing
C. Code review
D. Peer review

Answer: B

Explanation:
Regression testing is a type of software testing that ensures that a recent program or code change has not adversely affected existing features123 Regression testing is useful for checking if previously patched vulnerabilities have not been reintroduced by the new update.
Stress testing is a type of software testing that evaluates the performance and reliability of a system under extreme conditions, such as high load, limited resources, or concurrent users. Stress testing is not directly related to checking for vulnerabilities.
Code review is a process of examining the source code of a software program to find and fix errors, improve quality, and ensure compliance with standards and best practices. Code review can help prevent vulnerabilities from being introduced in the first place, but it does not verify that existing features are working as expected after a code change.
Peer review is a process of evaluating the work of another person or group of people, such as a research paper, a report, or a design. Peer review can provide feedback and suggestions for improvement, but it does not test the functionality or security of a software product.

NEW QUESTION 7
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

A. Implement privileged access management
B. Implement a risk management process
C. Implement multifactor authentication
D. Add more security resources to the environment

Answer: A

Explanation:
Implementing privileged access management (PAM) would be the best countermeasure to prevent the loss of customers' sensitive data due to a rise in cyberattackers seeking PHI (Protected Health Information). PAM is a solution that helps to control and monitor the access and use of privileged accounts, such as administrator or root accounts, that have elevated permissions or access to sensitive data. PAM can help prevent unauthorized or accidental use of privileged accounts by enforcing strict access policies, such as requiring approval, authentication, or auditing for each access request. PAM can also help rotate or expire the passwords of privileged accounts to reduce the risk of compromise2. PAM can help protect PHI from cyberattackers who may try to exploit privileged accounts to access or exfiltrate sensitive data.

NEW QUESTION 8
A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. VPC
C. Federation
D. VPN

Answer: D

Explanation:
A VPN is a secure network connection that allows users to access their private corporate networks over the internet, while keeping the connection encrypted and secure. This makes it an ideal solution for providing the development team with secure connectivity from the corporate network to a three-tier cloud environment.
https://www.comptia.org/content/virtual-private-networks

NEW QUESTION 9
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 10
Which of the following is the greatest security concern regarding ICS?

A. The involved systems are generally hard to identify.
B. The systems are configured for automatic updates, leading to device failure.
C. The systems are oftentimes air gapped, leading to fileless malware attacks.
D. Issues on the systems cannot be reversed without rebuilding the systems.

Answer: D

Explanation:
Industrial control systems (ICS) are systems that monitor and control physical processes, such as power generation, water treatment, manufacturing, and transportation. ICS are often critical for public safety and national security, and therefore a prime target for cyberattacks. One of the greatest security concerns regarding ICS is that issues on the systems cannot be reversed without rebuilding the systems. This means that any damage or disruption caused by an attack can have long-lasting and catastrophic consequences for the physical infrastructure and human lives. The other options are not true or not specific to ICS. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 13;
https://www.us-cert.gov/ics/What-are-Industrial-Control-Systems

NEW QUESTION 10
A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR
B. Port security
C. NAC
D. Segmentation

Answer: A

Explanation:
EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance requirements across all devices .

NEW QUESTION 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 v
D. blue team
E. 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

NEW QUESTION 16
A company's threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken. Which of the following is the next step the company should take to ensure any future issues are remediated?

A. Require support teams to develop a corrective control that ensures security failures are addressed once they are identified.
B. Require support teams to develop a preventive control that ensures new systems are built with the required security configurations.
C. Require support teams to develop a detective control that ensures they continuously assess systems for configuration errors.
D. Require support teams to develop a managerial control that ensures systems have a documented configuration baseline.

Answer: A

Explanation:
Requiring support teams to develop a corrective control that ensures security failures are addressed once they are identified is the best step to prevent future issues from being remediated. Corrective controls are actions or mechanisms that are implemented after a security incident or failure has occurred to fix or restore the normal state of the system or network. Corrective controls can include patching, updating, repairing, restoring, or reconfiguring systems or components that were affected by the incident or failure .

NEW QUESTION 20
A manufacturing company has joined the information sharing and analysis center for its sector. As a benefit, the company will receive structured loC data contributed by other members. Which of the following best describes the utility of this data?

A. Other members will have visibility into Instances o' positive loC identification within me manufacturing company's corporate network.
B. The manufacturing company will have access to relevant malware samples from all other manufacturing sector members.
C. Other members will automatically adjust their security postures lo defend the manufacturing company's processes.
D. The manufacturing company can automatically generate security configurations for all of Its Infrastructure.

Answer: B

Explanation:
This best describes the utility of the structured loC data contributed by other members of the information sharing and analysis center (ISAC) for its sector. loC stands for indicator of compromise, which is a piece of information that suggests a potential intrusion or attack, such as an IP address, a file hash, a domain name, or a malware signature. By sharing loC data, the ISAC members can benefit from each other’s threat intelligence and improve their security defenses.

NEW QUESTION 21
A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines. Which of the following solutions would be best to accomplish this goal?

A. WPA2 for W1F1 networks
B. NAC with 802.1X implementation
C. Extensible Authentication Protocol
D. RADIUS with challenge/response

Answer: B

Explanation:
This solution is the best to accomplish the goal of blocking all non-corporate managed machines from connecting to the internal network. NAC stands for network access control, which is a method of enforcing policies and rules on network devices based on their identity, role, location, and other attributes. 802.1X is a standard for port-based network access control, which authenticates devices before granting them access to a network port or wireless access point.

NEW QUESTION 22
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy

Answer: B

Explanation:
Threat intelligence can be used to identify likely attack scenarios within an organization based on the organization’s specific vulnerabilities, assets, and threat

landscape. Threat intelligence can help security teams anticipate and prepare for potential attacks, as well as detect and respond to ongoing attacks more effectively1. Threat intelligence can also provide insights into the threat actors, their motivations, and their tactics, techniques, and procedures (TTPs)2.

NEW QUESTION 24
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 25
An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following will the analyst most likely do next given the requirements?

A. Request to route traffic through a secondary firewall
B. Check for change tickets.
C. Perform a credentialed scan
D. Request an exception to the uptime policy.

Answer: B

Explanation:
The analyst should check for change tickets as the next step, given that the firewall is reporting different firmware versions on scans than were reported in previous scans. Change tickets are records of any authorized changes made to a system or a network, such as updating firmware, installing patches, or modifying configurations. Checking for change tickets can help verify if the firmware change was intentional and approved, or if it was unauthorized or malicious.

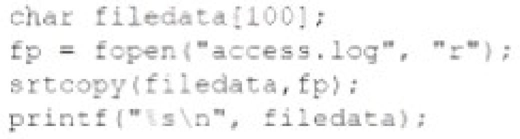
NEW QUESTION 27
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

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 32
An internally developed file-monitoring system identified the following except as causing a program to crash often:



```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

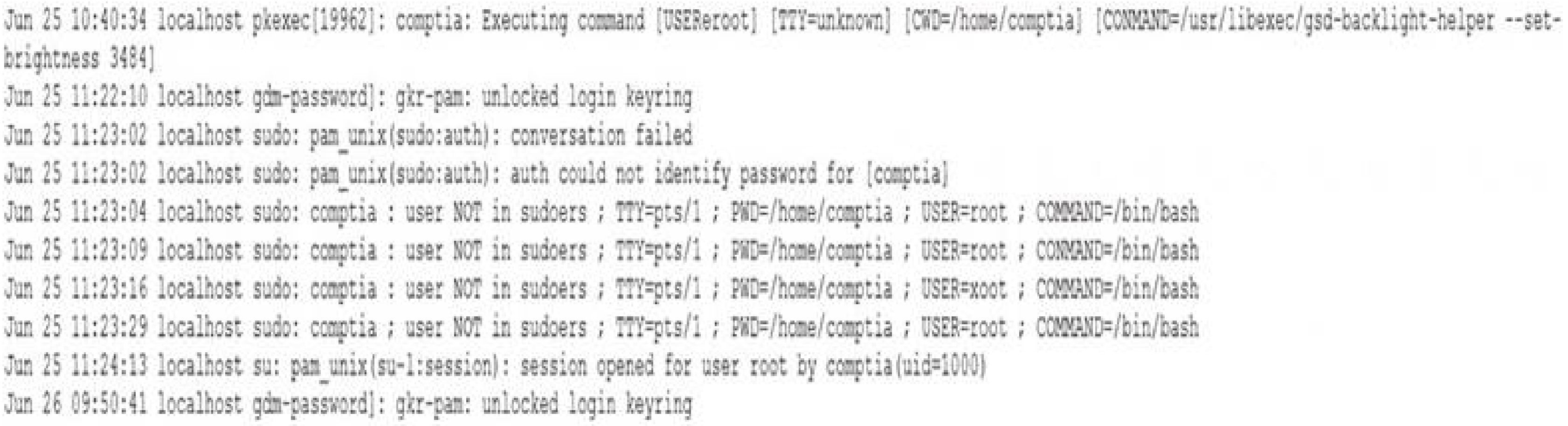
Which of the following should a security analyst recommend to fix the issue?

A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer

Answer: B

Explanation:
The security analyst should recommend replacing the strcpy function with a safer alternative. The strcpy function is a C library function that copies a string from one buffer to another. However, this function does not check the size of the destination buffer, which can lead to buffer overflow vulnerabilities if the source string is longer than the destination buffer. Buffer overflow vulnerabilities can allow attackers to execute arbitrary code or crash the program. A safer alternative to strcpy is strncpy, which limits the number of characters copied to the size of the destination buffer.

NEW QUESTION 36
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 ; COMMAND=/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/

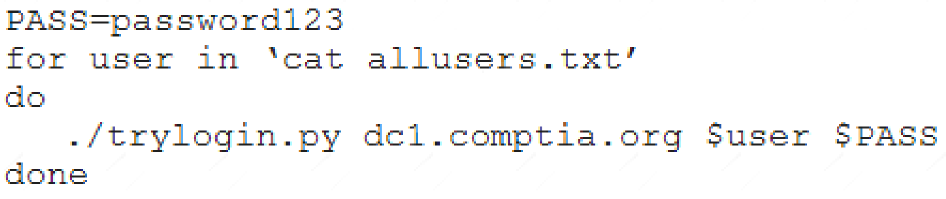
NEW QUESTION 41
An analyst is working on a method to allow secure access to a highly sensi-tive server. The solution must allow named individuals remote access to data contained on the box and must limit access to a single IP address. Which of the following solutions would best meet these requirements?

A. Jump box
B. Software-defined networking
C. VLAN
D. ACL

Answer: A

Explanation:
A jump box is a secure computer that can be used to access a remote server or network. It acts as an intermediary between the user and the target system, and can limit access to specific IP addresses. A jump box can also provide logging and auditing of the user's actions on the remote system. A jump box is a common solution for accessing highly sensitive servers or networks1.

NEW QUESTION 44
When investigating a compromised system, a security analyst finds the following script in the /tmp directory:



```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Answer: B

Explanation:
https://owasp.org/www-community/attacks/Password_Spraying_Attack
A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

NEW QUESTION 47
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 51
Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: D

Explanation:
Understanding assets and categories of assets is most important when developing a threat hunting program. Assets are anything that have value to an organization, such as data, systems, networks, applications, devices, people, processes, or reputation. Categories of assets are groups of assets that share common characteristics or attributes, such as type, function, location, owner, or criticality. Understanding assets and categories of assets can help to identify and prioritize the potential targets and impact of threats in an organization. Understanding assets and categories of assets can also help to determine and apply appropriate security controls and measures for each asset or category. Understanding assets and categories of assets can also help to collect and analyze relevant data and indicators for each asset or category during threat hunting activities. Understanding penetration testing techniques (A) is not most important when developing a threat hunting program. Penetration testing techniques are methods or tools that are used to simulate attacks on a system or network to evaluate its security posture and identify vulnerabilities or weaknesses. Penetration testing techniques can help to validate and improve the security of an organization, but they are not directly related to threat hunting activities. Penetration testing techniques are reactive rather than proactive approaches to security. Understanding how to build correlation rules within a SIEM (B) is also not most important when developing a threat hunting program. Correlation rules are logic statements that define relationships or patterns between different events or data points in a system or network. A SIEM (Security Information and Event Management) is a software solution that collects, analyzes, and correlates data from various sources in an organization to provide security monitoring and alerting capabilities1. Correlation rules can help to detect and respond to known threats in an organization, but they are not sufficient for threat hunting activities. Correlation rules are based on predefined criteria rather than hypotheses or assumptions about unknown threats. Understanding security software technologies © is also not most important when developing a threat hunting program. Security software technologies are applications or programs that provide security functions or features for an organization, such as antivirus software, firewalls, encryption software, VPNs (Virtual Private Networks), etc2. Security software technologies can help to protect an organization from various threats, but they are not essential for threat hunting activities. Security software technologies are based on signatures or heuristics rather than indicators of compromise or behavioral analysis.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 53
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 incident3. Postmortem data correlation can help the security team to:

- Determine how the incident occurred and how it was detected and resolved
- 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

NEW QUESTION 54
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 55

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

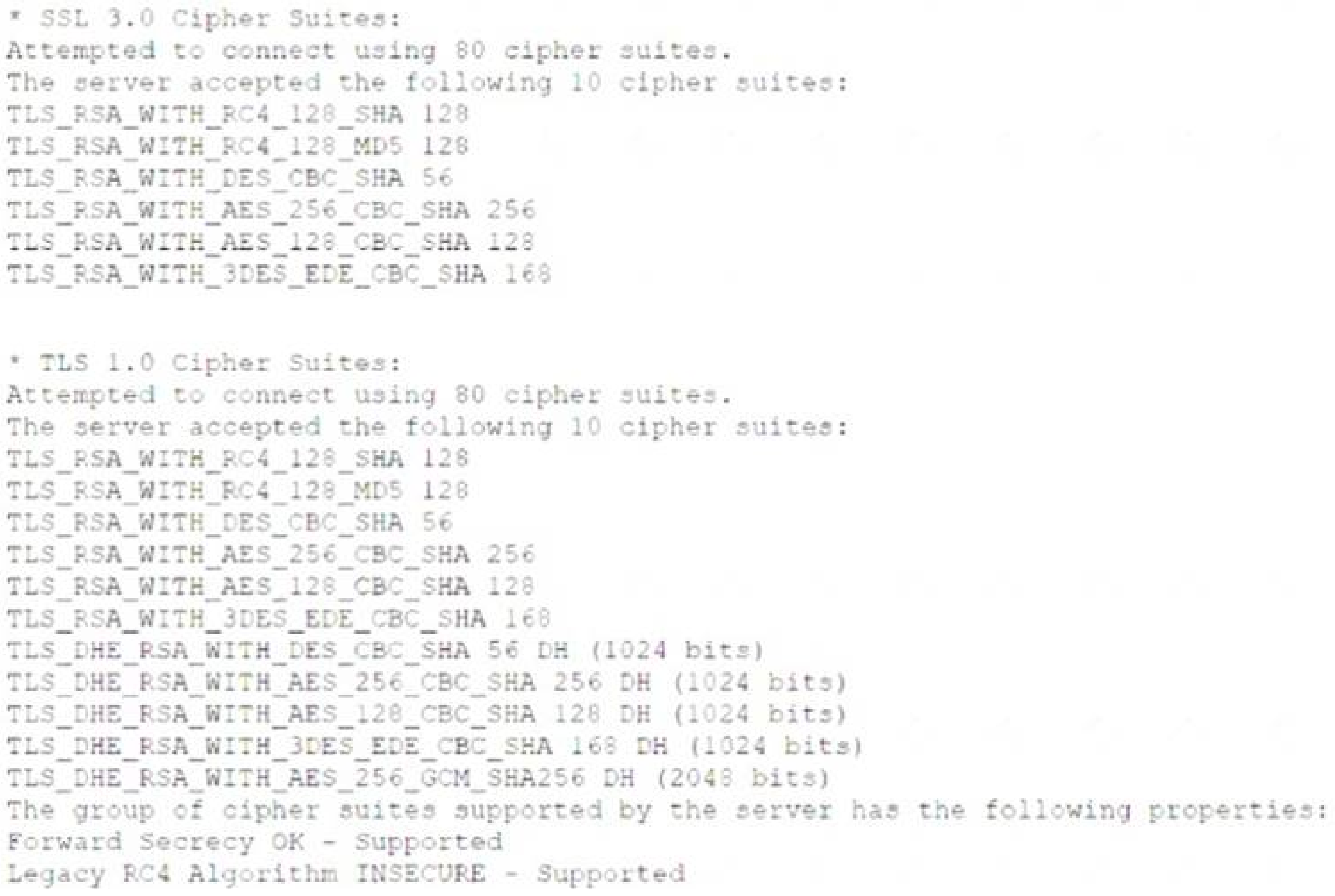
NEW QUESTION 59
An application developer needs help establishing a digital certificate for a new application. Which of the following illustrates a certificate management best practice?

A. Ensure the certificate Is applied to the certificate revocation list.
B. Ensure the certificate key algorithm is SHA-1 compliant.
C. Ensure the certificate is requested from a trusted CA.
D. Ensure the developer has self-signed the certificate.
E. Ensure the certificate key is less than 1028 bits long.

Answer: C

Explanation:
The best practice for establishing a digital certificate for a new application is to ensure the certificate is requested from a trusted CA. A CA stands for Certificate Authority, and it is an entity that issues and verifies digital certificates, which are electronic documents that contain a public key and a digital signature that prove the identity and authenticity of an application, a website, or a person. Requesting a certificate from a trusted CA can help ensure that the certificate is valid, secure, and recognized by other parties.

NEW QUESTION 62
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 66
A security analyst is concerned about sensitive data living on company file servers following a zero-day attack that nearly resulted in a breach of millions of customer records. The after action report indicates a lack of controls around the file servers that contain sensitive data. Which of the following DLP considerations would best help the analyst to classify and address the sensitive data on the file servers?

A. Implement a CASB device and connect the SaaS applications.
B. Deploy network DLP appliances pointed to all file servers.
C. Use data-at-rest scans to locate and identify sensitive data.
D. Install endpoint DLP agents on all computing resources.

Answer: C

Explanation:
Use data-at-rest scans to locate and identify sensitive data. This option is the best DLP consideration for addressing the sensitive data on the file servers. Data-at-rest scans are performed on data that is stored on a device or a network, such as file servers, and can help identify and classify sensitive data based on predefined policies or rules. The other options are not relevant for this scenario, as they either deal with data in transit (network DLP appliances), data in use (endpoint DLP agents), or cloud-based data (CASB device).

NEW QUESTION 67
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
D. Meet with the senior management team to determine if funding is available for recommended solutions.

Answer: C

Explanation:
A good approach for modeling the client’s attack surface is to look at attacks against similar industry peers and assess the probability of the same attacks happening. This can help the consultant to identify the most relevant and likely threats for the client based on their industry sector, size, location, and other factors. This can also help the consultant to prioritize the most critical risks and recommend appropriate mitigation strategies. Asking for external scans from industry peers (A) may not be feasible or reliable, as industry peers may not share their scan results or have different security configurations and vulnerabilities than the client. Discussing potential tools the client can purchase (B) may not be effective, as tools alone cannot reduce the likelihood of an attack without proper implementation and management. Meeting with senior management team (D) may not be helpful, as funding is not directly related to modeling the attack surface and may depend on other factors such as budget constraints and risk appetite.

NEW QUESTION 69
An organization wants to implement controls for protecting private information at rest. Which of the following would meet the organization's need?

A. Non-disclosure agreements
B. Retention policies
C. Data minimization
D. Encryption

Answer: D

Explanation:
The correct answer is D. Encryption. Encryption is a technical control that transforms data into an unreadable format using a secret key or algorithm. Encryption can protect data at rest by preventing unauthorized access, modification, or exfiltration of the data. Encryption can also protect data in transit and in use, depending on the type and level of encryption applied1.

NEW QUESTION 74
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 78
A new variant of malware is spreading on the company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

A. Implement a sinkhole with a high entropy level
B. Disable TCP/53 at the parameter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion

Answer: A

Explanation:
A sinkhole is a technique that redirects malicious network traffic to a controlled destination, such as a fake server or a black hole. A sinkhole can be used to stop malicious communications with a command-and-control server by preventing the malware from reaching its intended destination. A high entropy level means that the sinkhole can generate random domain names that match the changing domain name used by the malware for callback. Blocking TCP/443 at the edge router, disabling TCP/53 at the perimeter firewall, or configuring the DNS forwarders to use recursion are other possible actions that could stop malicious communications, but they could also disrupt legitimate services that use those protocols or settings. Reference: https://www.cisco.com/c/en/us/about/security-center/dns-sinkholing.html

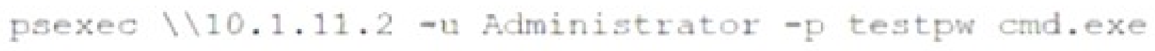
NEW QUESTION 79
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

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 hardware2
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.

NEW QUESTION 80
While reviewing system logs, a network administrator discovers the following entry:



```
psexec \\10.1.11.2 -u Administrator -p testpw cmd.exe
```

Which of the following occurred?

A. An attempt was made to access a remote workstation.
B. The PsExec services failed to execute.
C. A remote shell failed to open.
D. A user was trying to download a password file from a remote system.

Answer: D

Explanation:
The output shows an entry from a system log that indicates a user was trying to download a password file from a remote system using PsExec. PsExec is a command-line tool that allows users to execute processes on remote systems. The entry shows that the user “administrator” tried to run PsExec with the following parameters: \192.168.1.100 -u administrator -p P@ssw0rd -c cmd.exe /c type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt This means that the user tried to connect to the remote system with IP address 192.168.1.100 using the username “administrator” and password “P@ssw0rd”, copy cmd.exe to the remote system, and execute it with the command “type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt”. This command attempts to read the SAM file, which contains hashed passwords of local users, and write it to a file on another system with IP address 192.168.1.101. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

NEW QUESTION 83
A new prototype for a company's flagship product was leaked on the internet As a result, the management team has locked out all USB drives Optical drive writers are not present on company computers The sales team has been granted an exception to share sales presentation files with third parties Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging
B. Device encryption
C. Data loss prevention
D. SIEMlogs

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 SIEM system can help the IT team to determine which devices are USB enabled by querying the log data for events related to USB device insertion, removal, or usage. The other options are not relevant or effective 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 88
A systems administrator believes a user's workstation has been compromised. The workstation's performance has been lagging significantly for the past several hours. The administrator runs the task list
/ v command and receives the following output:

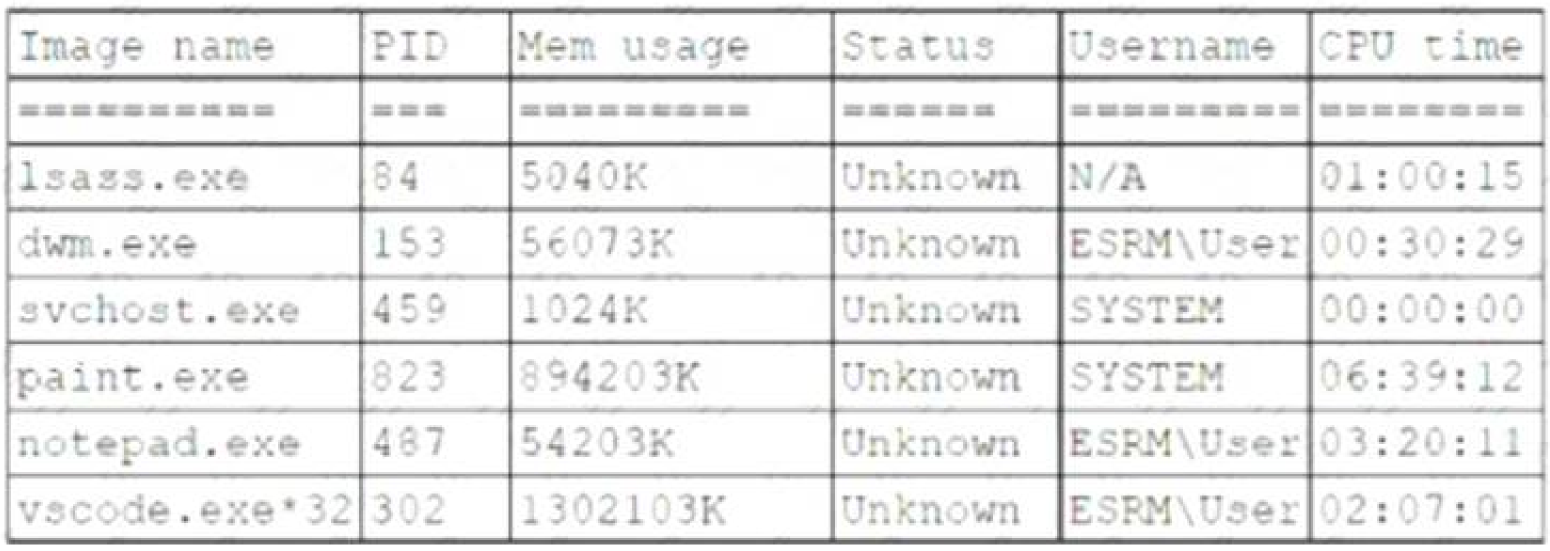


Image name	PID	Mem usage	Status	Username	CPU time
==========	===	=========	======	=========	========
lsass.exe	84	5040K	Unknown	N/A	01:00:15
dwm.exe	153	56073K	Unknown	ESRM\User	00:30:29
svchost.exe	459	1024K	Unknown	SYSTEM	00:00:00
paint.exe	823	894203K	Unknown	SYSTEM	06:39:12
notepad.exe	487	54203K	Unknown	ESRM\User	03:20:11
vscode.exe*32	302	1302103K	Unknown	ESRM\User	02:07:01

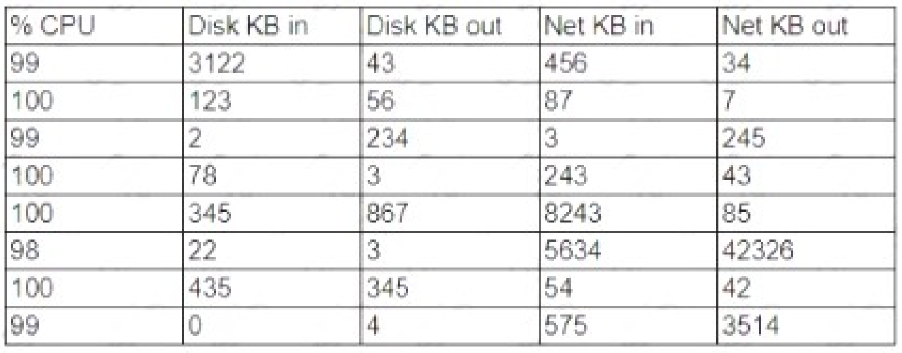
Which of the following should a security analyst recognize as an indicator of compromise?

A. dwm.exe being executed under the user context
B. The high usage of vscod
C. exe * 32
D. The abnormal behavior of paint.exe
E. svchost.exe being executed as SYSTEM

Answer: B

Explanation:
The tasklist command is used to display a list of all running processes on a system. In this output, the security analyst should recognize the high memory usage (1302103K) of vscode.exe * 32, which is an indication that this process is consuming a large amount of system resources. This could be a sign that the system has been compromised, as malware often uses system resources to perform malicious activities.

NEW QUESTION 90
A security analyst is reviewing the following server statistics:



% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?

A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

Explanation:
Resource exhaustion is most likely occurring on the server. Resource exhaustion is a condition where a system runs out of resources, such as CPU, memory, disk space, or network bandwidth, due to excessive demand or consumption by one or more processes. Resource exhaustion can cause performance degradation, system instability, or denial-of-service. The server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%. These indicate that the server is under heavy load and has little or no resources available to handle incoming requests or perform other tasks.

NEW QUESTION 92
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-s

NEW QUESTION 96
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the first steps to confirm and respond to the incident? (Select two).

A. Pause the virtual machine.
B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.
D. Remove the NIC from the virtual machine.
E. Review host hypervisor log of the virtual machine.
F. Execute a migration of the virtual machine.

Answer: AC

Explanation:
These steps are the best to confirm and respond to the incident because they preserve the state of the compromised server for further analysis and evidence collection. Pausing the virtual machine prevents any further changes or damage by the attacker, while taking a snapshot creates a copy of the virtual machine's memory and disk contents.

NEW QUESTION 98
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 101
A company is setting up a small, remote office to support five to ten employees. The company's home office is in a different city, where the company uses a cloud service provider for its business applications and a local server to host its data. To provide shared access from the remote office to the local server and the business applications, which of the following would be the easiest and most secure solution?

A. Use a VPC to host the company's data and keep the current solution for the business applications.
B. Use a new server for the remote office to host the data and keep the current solution for the business applications.
C. Use a VDI for the home office and keep the current solution for the business applications.
D. Use a VPN to access the company's data in the home office and keep the current solution for the business applications.

Answer: D

Explanation:
The correct answer is D. Use a VPN to access the company's data in the home office and keep the current solution for the business applications. A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN can allow users to access resources on a remote network, such as a server, as if they were on the same local network. A VPN can provide shared access from the remote office to the company's data in the home office, while maintaining security and privacy1.

NEW QUESTION 104
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. An accounting supervisor's laptop that is connected to the VPN
D. The laptop of the vice president that is on the corporate LAN

Answer: D

Explanation:
The laptop of the vice president that is on the corporate LAN should be investigated first. According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, when prioritizing security alerts, the analyst should prioritize assets based on the potential impact of a successful attack or compromise. Therefore, the laptop of the vice president, which is connected to the corporate LAN, should be investigated first, as it has the highest potential impact.

NEW QUESTION 106
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

A. Analysis and production
B. Processing and exploitation
C. Dissemination and evaluation
D. Data collection
E. Planning and direction

Answer: B

Explanation:
Processing and exploitation is the step in the intelligence cycle that involves converting raw data into a format that can be used for analysis and producing intelligence products that can be disseminated to consumers. The security analyst is performing this step by correlating, ranking, and enriching raw data into a report. Analysis and production, dissemination and evaluation, data collection, and planning and direction are other steps in the intelligence cycle, but they do not match the description of the security analyst’s task. Reference:
https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-cycle.htm

NEW QUESTION 107
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 109
An organization needs to secure sensitive data on its critical networks by implementing controls to mitigate APTs. The current policy does not provide any guidance or processes that support the mitigation of APTs. Which of the following technologies should the organization implement lo secure sensitive data? (Select two).

A. WAF
B. VPN
C. VPC
D. IPS
E. SIEM
F. SSO

Answer: DE

Explanation:
IPS and SIEM are technologies that can help secure sensitive data on critical networks by implementing controls to mitigate APTs. IPS stands for Intrusion Prevention System, and it is a device or software that monitors network traffic and blocks or prevents malicious packets or activities based on predefined rules or signatures. IPS can help detect and stop APTs that may try to exploit vulnerabilities or bypass security controls on critical networks. SIEM stands for Security Information and Event Management, and it is a system that collects, correlates, analyzes, and reports security data from various sources, such as logs, alerts, events, etc. SIEM can help identify and respond to APTs that may exhibit anomalous or suspicious behavior patterns on critical networks.

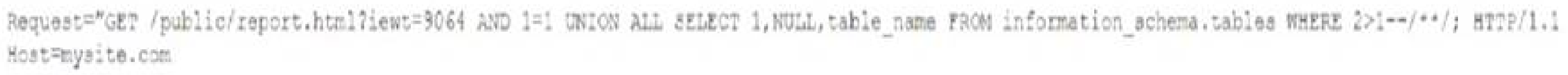
NEW QUESTION 113
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
D. Unsupervised algorithms produce more false positive
E. Than supervised algorithms.

Answer: B

Explanation:
Supervised and unsupervised machine-learning algorithms are two types of machine-learning methods that are used in cybersecurity applications. Machine learning is a branch of artificial intelligence that enables systems to learn from data and improve their performance without explicit programming.
Supervised machine-learning algorithms are trained on labeled data, which means that each data point has a known outcome or class. Supervised algorithms learn to map input data to output data by finding patterns or rules from the training data. Supervised algorithms require security analyst feedback to provide labels for the data and evaluate the accuracy of the algorithm’s predictions. Examples of supervised machine-learning algorithms are classification and regression.
Unsupervised machine-learning algorithms are trained on unlabeled data, which means that each data point has no known outcome or class. Unsupervised algorithms learn to discover hidden structures or patterns from the data without any guidance or feedback. Unsupervised algorithms do not require security analyst feedback, as they do not rely on predefined labels or outcomes. Examples of unsupervised machine-learning algorithms are clustering and anomaly detection.

NEW QUESTION 117
A security analyst is reviewing WAF alerts and sees the following request:



```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?

A. SQL injection
B. LDAP injection
C. Command injection
D. Denial of service

Answer: A

Explanation:
The attack is a SQL injection attack. SQL injection is a type of attack that exploits a security vulnerability in an application's software that allows user input to be executed as SQL commands by the underlying database3. SQL injection can enable an attacker to perform various malicious actions on the database, such as reading, modifying, deleting or creating data; executing commands; or bypassing authentication. The request shows that the attacker has entered a malicious SQL statement in the username parameter that attempts to drop (delete) all tables in the database.

NEW QUESTION 118
A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Create an IPS rule to block the subnet.
B. Sinkhole the IP address.
C. Create a firewall rule to block the IP address.
D. Close all unnecessary open ports.

Answer: C

Explanation:
A firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules. Creating a firewall rule to block the IP address that is scanning the organization's environment is an effective way to stop this activity and prevent potential attacks. Creating an IPS rule to block the subnet, sinkholing the IP address, or closing all unnecessary open ports are other possible actions, but they are not as specific or efficient as creating a firewall rule to block the IP address. Reference: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/firewall.html

NEW QUESTION 123
A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

A. Static analysis
B. Stress testing
C. Code review
D. User acceptance testing

Answer: D

Explanation:
User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback . User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders.

NEW QUESTION 127
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts

Answer: A

Explanation:
System timeline reconstruction is a forensic analysis technique that involves creating a chronological record of events that occurred on a system based on various sources of evidence such as log files, registry entries, file timestamps, network traffic, etc. System timeline reconstruction can provide information about when and how the machine was compromised and where the malware is located by showing when suspicious activities or changes took place on the system, such as unauthorized access attempts, file creation or modification, process execution, network connections, etc.

NEW QUESTION 131
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 135
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

A. vulnerability scanning.
B. threat hunting.
C. red learning.
D. penetration testing.

Answer: B

Explanation:
Threat hunting is a proactive process of searching for signs of malicious activity or compromise within a system or network, by using hypotheses, indicators of compromise, and analytical tools. Threat hunting can help improve detection capabilities by identifying unknown threats, uncovering gaps in security controls, and providing insights for remediation and prevention. Vulnerability scanning (A) is a reactive process of scanning systems or networks for known vulnerabilities or weaknesses that can be exploited by attackers. It can help identify and prioritize vulnerabilities, but not proactively hunt for threats. Red teaming © is a simulated attack on a system or network by a group of ethical hackers who act as adversaries and try to breach security controls. It can help test the effectiveness of security defenses and response capabilities, but not proactively hunt for threats. Penetration testing (D) is similar to red teaming, but with a more defined scope and objective. It can help evaluate the security of a system or network by simulating real-world attacks and exploiting vulnerabilities, but not proactively hunt for threats.
References: : https://www.techopedia.com/definition/33297/threat-hunting : https://www.techopedia.com/definition/4160/web-application-security-scanner-was : https://www.techopedia.com/definition/32694/red-teaming :
https://www.techopedia.com/definition/13493/penetration-testing

NEW QUESTION 136
A threat feed disclosed a list of files to be used as an IoC for a zero-day vulnerability. A cybersecurity analyst decided to include a custom lookup for these files on the endpoint's log-in script as a mechanism to:

A. automate malware signature creation.
B. close the threat intelligence cycle loop.
C. generate a STIX object for the TAXII server
D. improve existing detection capabilities.

Answer: D

Explanation:
The analyst decided to include a custom lookup for these files on the endpoint’s log-in script as a mechanism to improve existing detection capabilities, by checking if any of these files are present on the endpoints during log-in. This can help identify any compromised endpoints that may have been infected by the zero-day vulnerability, and alert the analyst for further investigation or response.

NEW QUESTION 138
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 142
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 146
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 151
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 153
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?

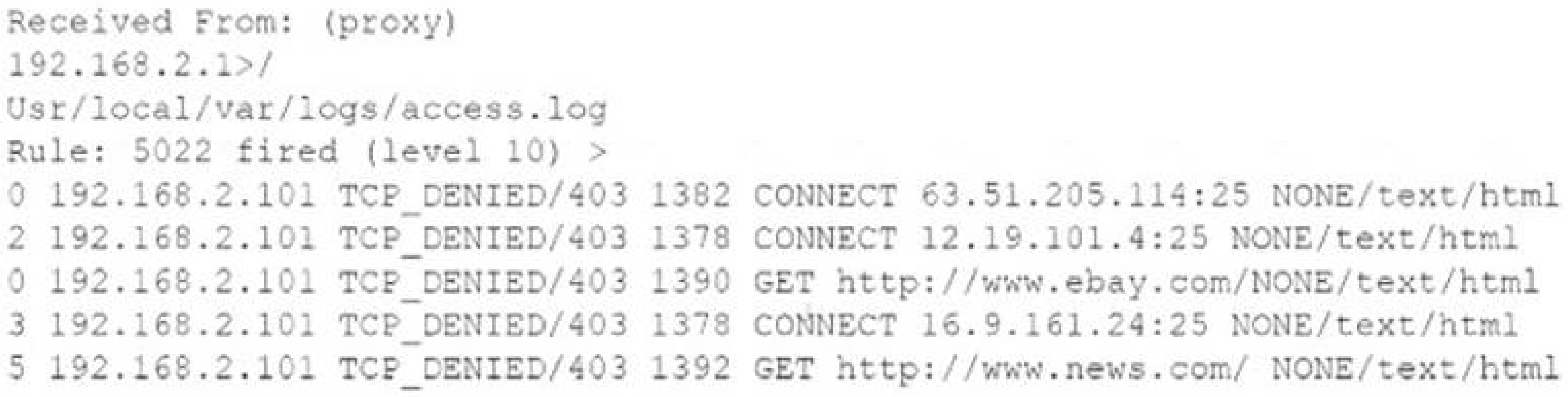
A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server
C. Implement input validation
D. Run a static code scan

Answer: C

Explanation:
In this scenario, the issue is related to manipulation of the public-facing web form, indicating that attackers might be altering the prices before submitting the form. One of the best ways to prevent such attacks is to implement input validation, which can help ensure that the data submitted to the web form is correct, complete,

and in the expected format. Input validation can also help prevent SQL injection and other types of web-based attacks.

NEW QUESTION 158
A security analyst notices the following proxy log entries:



```
Received From: (proxy)
192.168.2.1>/
Usr/local/var/logs/access.log
Rule: 5022 fired (level 10) >
0 192.168.2.101 TCP_DENIED/403 1382 CONNECT 63.51.205.114:25 NONE/text/html
2 192.168.2.101 TCP_DENIED/403 1378 CONNECT 12.19.101.4:25 NONE/text/html
0 192.168.2.101 TCP_DENIED/403 1390 GET http://www.ebay.com/NONE/text/html
3 192.168.2.101 TCP_DENIED/403 1378 CONNECT 16.9.161.24:25 NONE/text/html
5 192.168.2.101 TCP_DENIED/403 1392 GET http://www.news.com/ NONE/text/html
```

Which of the following is the user attempting to do based on the log entries?

A. Use a DoS attack on external hosts.
B. Exfiltrate data.
C. Scan the network.
D. Relay email.

Answer: C

Explanation:
Scanning the network is what the user is attempting to do based on the log entries. The log entries show that the user is sending ping requests to various IP addresses on different ports using a proxy server. Ping requests are a common network diagnostic tool that can be used to test network connectivity and latency by sending packets of data and measuring their response time. However, ping requests can also be used by attackers to scan the network and discover active hosts, open ports, or potential vulnerabilities .

NEW QUESTION 160
According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?

A. Delete the vulnerable section of the code immediately.
B. Create a custom rule on the web application firewall.
C. Validate user input before execution and interpretation.
D. Use parameterized queries.

Answer: C

Explanation:
Validating user input before execution and interpretation can help to prevent dynamic code evaluation script injection vulnerabilities by checking and filtering any malicious input from the user that may contain code or commands. Dynamic code evaluation script injection is a type of vulnerability that occurs when an application accepts user input and executes or interprets it as part of its own code without proper validation or sanitization. This can allow an attacker to inject arbitrary code or commands into the application and execute them with the same privileges as the application . Validating user input before execution and interpretation can help to ensure that the 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 .

NEW QUESTION 162
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

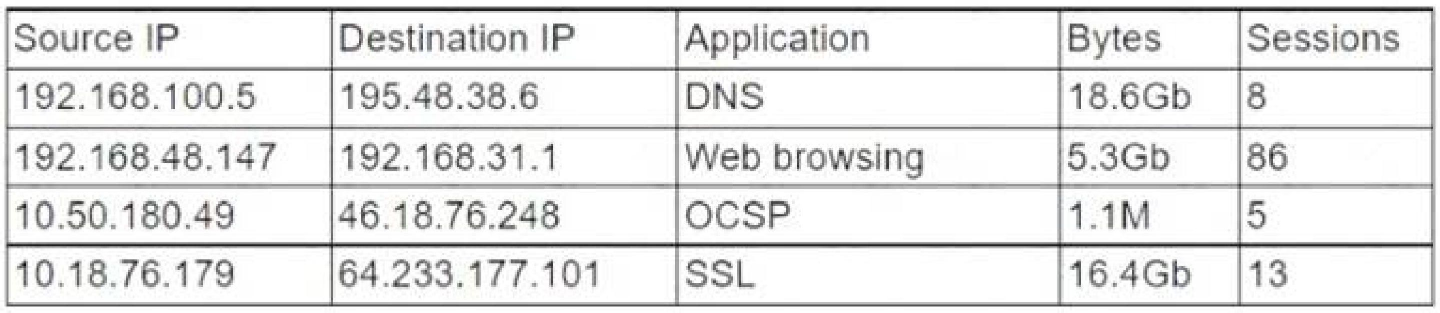
NEW QUESTION 167
Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

A. APTs' passion for social justice will make them ongoing and motivated attackers.
B. APTs utilize methods and technologies differently than other threats
C. APTs are primarily focused on financial gam and are widely available over the internet.
D. APTs lack sophisticated methods, but their dedication makes them persistent.

Answer: B

Explanation:
APTs utilize methods and technologies differently than other threats. APTs stand for Advanced Persistent Threats, and they are sophisticated and stealthy attacks that target specific organizations or networks over a long period of time, often with political or financial motives. APTs utilize methods and technologies differently than other threats, such as using custom-made malware, exploiting zero-day vulnerabilities, leveraging social engineering techniques, or employing multiple vectors of attack. APTs can also evade detection by existing security tools or controls, by using encryption, obfuscation, proxy servers, or other techniques to hide their activities or communications.

NEW QUESTION 168
A security analyst is reviewing a firewall usage report that contains traffic generated over the last 30 minutes in order to locate unusual traffic patterns:



Source IP	Destination IP	Application	Bytes	Sessions
192.168.100.5	195.48.38.6	DNS	18.6Gb	8
192.168.48.147	192.168.31.1	Web browsing	5.3Gb	86
10.50.180.49	46.18.76.248	OCSP	1.1M	5
10.18.76.179	64.233.177.101	SSL	16.4Gb	13

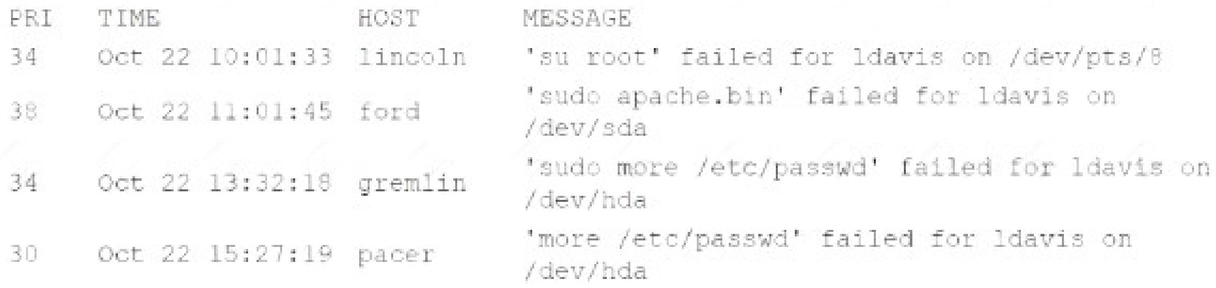
Which of the following source IP addresses does the analyst need to investigate further?

A. 10.18.76.179
B. 10.50.180.49
C. 192.168.48.147
D. 192.168.100.5

Answer: B

Explanation:
The security analyst needs to investigate further the source IP address 10.50.180.49. This IP address belongs to a private network that is not routable on the internet. However, the firewall usage report shows that this IP address has sent traffic to an external destination on port 443 (HTTPS). This could indicate that the IP address is spoofed or compromised by an attacker who is using it to exfiltrate data or communicate with a command-and-control server.

NEW QUESTION 171
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 175
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 .

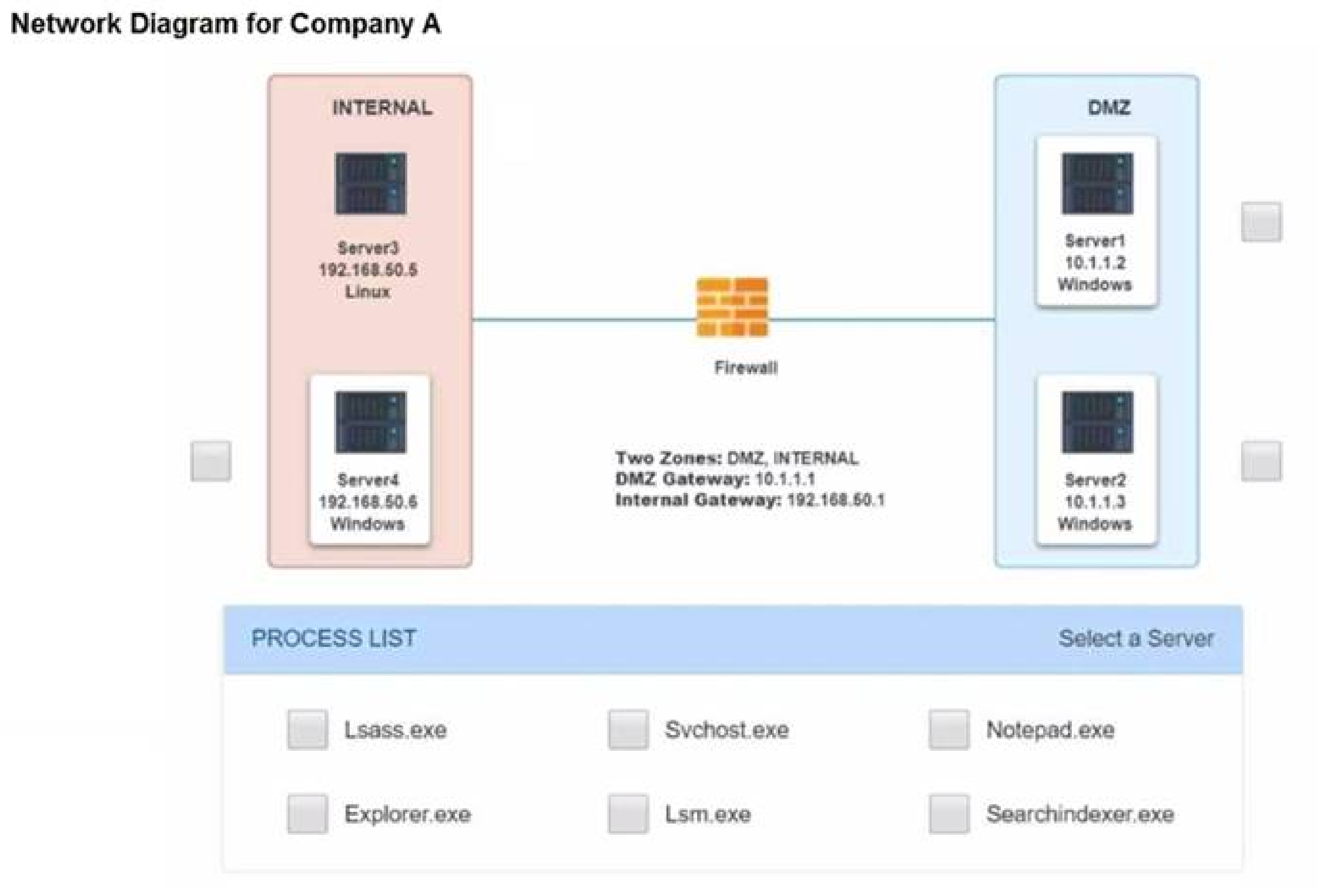
NEW QUESTION 180
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

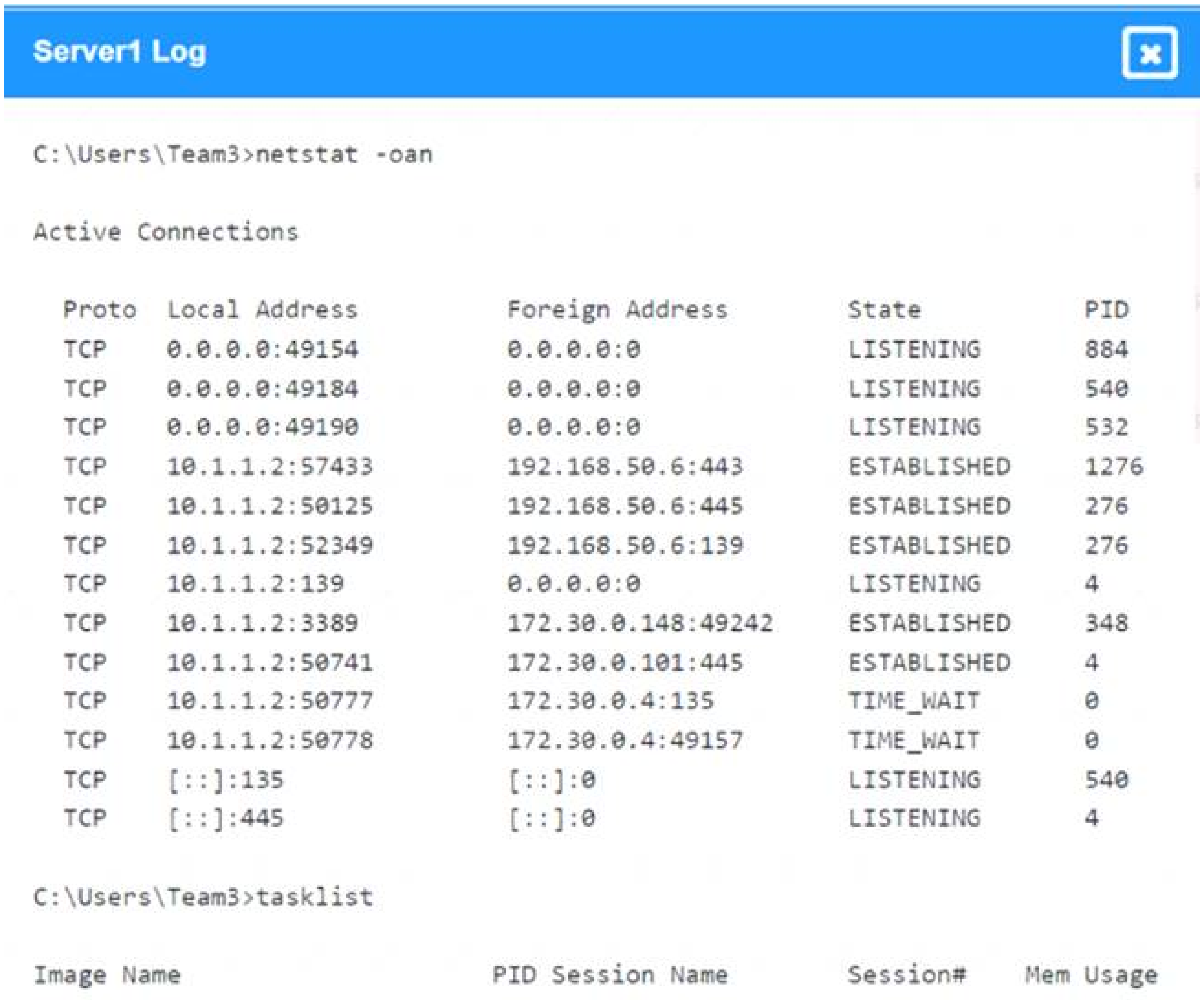
A. The extended support mitigates any risk associated with the software.
B. The extended support contract changes this vulnerability finding to a false positive.
C. The company is transferring the risk for the vulnerability to the software vendor.
D. The company is accepting the inherent risk of the vulnerability.

Answer: C

Explanation:
The company is transferring the risk for the vulnerability to the software vendor. Risk transfer is a risk treatment strategy that involves shifting the potential loss or impact of a risk to a third party, such as an insurance company or a vendor. Risk transfer does not eliminate the risk, but it reduces the organization’s exposure or liability for the risk1. In this scenario, the company is transferring the risk for the vulnerability in the out-of-support database software to the software vendor by signing an extended support contract. The extended support contract means that the software vendor will continue to provide security patches and updates for the software until the company can complete the software update. This reduces the likelihood and impact of a potential exploit of the vulnerability.

NEW QUESTION 184
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one Of the servers may be malware.
INSTRUCTIONS
Servers 1 , 2, and 4 are clickable. Select the Server and the process that host the malware.





Server1 Log

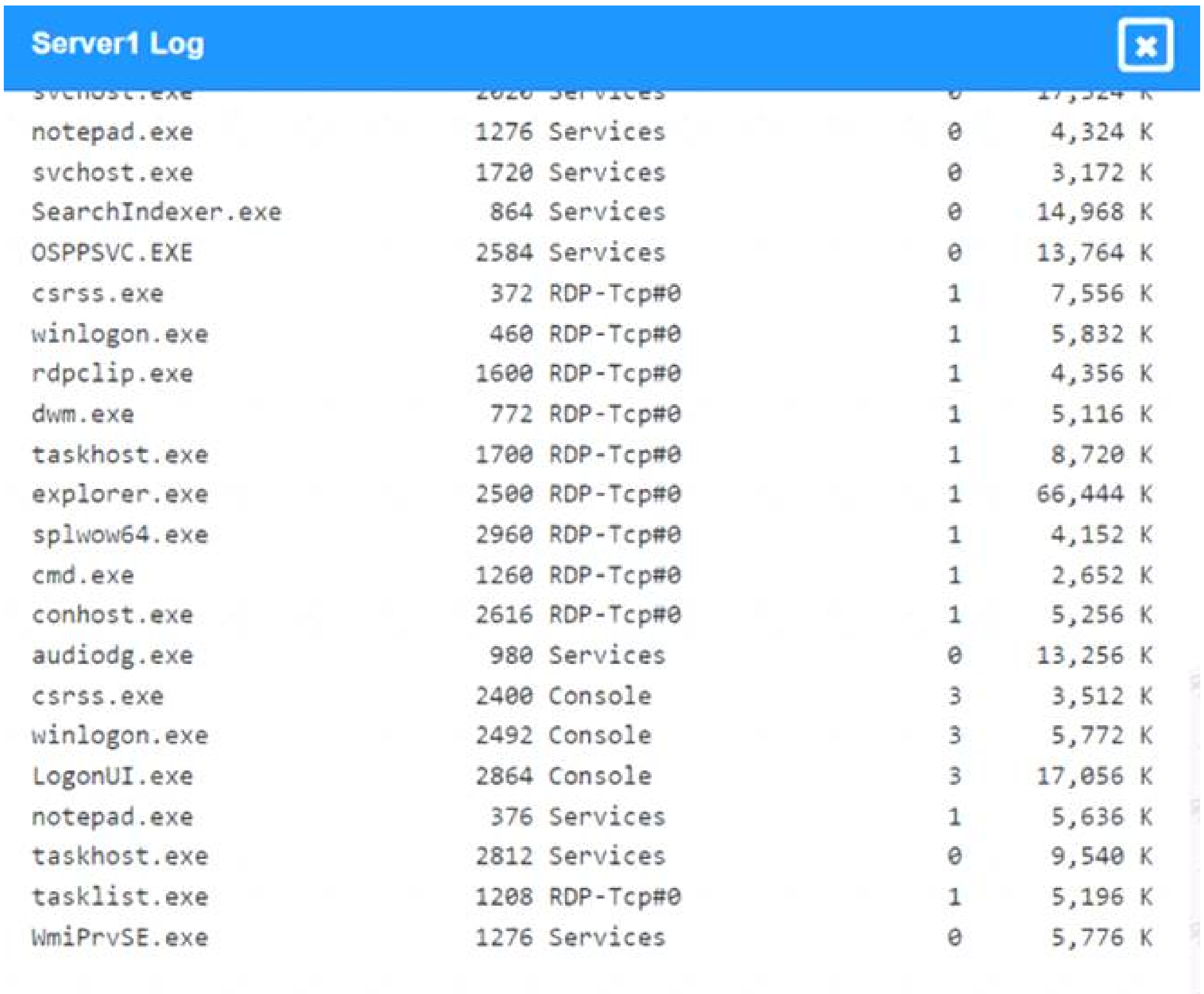
```
C:\Users\Team3>netstat -oan

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:49184          0.0.0.0:0              LISTENING       540
  TCP    0.0.0.0:49190          0.0.0.0:0              LISTENING       532
  TCP    10.1.1.2:57433         192.168.50.6:443       ESTABLISHED     1276
  TCP    10.1.1.2:50125         192.168.50.6:445       ESTABLISHED     276
  TCP    10.1.1.2:52349         192.168.50.6:139       ESTABLISHED     276
  TCP    10.1.1.2:139           0.0.0.0:0              LISTENING       4
  TCP    10.1.1.2:3389          172.30.0.148:49242     ESTABLISHED     348
  TCP    10.1.1.2:50741         172.30.0.101:445       ESTABLISHED     4
  TCP    10.1.1.2:50777         172.30.0.4:135         TIME_WAIT       0
  TCP    10.1.1.2:50778         172.30.0.4:49157       TIME_WAIT       0
  TCP    [::]:135               [::]:0                 LISTENING       540
  TCP    [::]:445               [::]:0                 LISTENING       4

C:\Users\Team3>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
```



Server1 Log

```
svchost.exe                   2020 Services                   0     17,324 K
notepad.exe                   1276 Services                   0      4,324 K
svchost.exe                   1720 Services                   0      3,172 K
SearchIndexer.exe              864 Services                   0     14,968 K
OSPPSVC.EXE                   2584 Services                   0     13,764 K
csrss.exe                      372 RDP-Tcp#0                  1      7,556 K
winlogon.exe                   460 RDP-Tcp#0                  1      5,832 K
rdpclip.exe                   1600 RDP-Tcp#0                  1      4,356 K
dwm.exe                        772 RDP-Tcp#0                  1      5,116 K
taskhost.exe                  1700 RDP-Tcp#0                  1      8,720 K
explorer.exe                  2500 RDP-Tcp#0                  1     66,444 K
splwow64.exe                  2960 RDP-Tcp#0                  1      4,152 K
cmd.exe                       1260 RDP-Tcp#0                  1      2,652 K
conhost.exe                   2616 RDP-Tcp#0                  1      5,256 K
audiodg.exe                    980 Services                   0     13,256 K
csrss.exe                     2400 Console                    3      3,512 K
winlogon.exe                  2492 Console                    3      5,772 K
LogonUI.exe                   2864 Console                    3     17,056 K
notepad.exe                    376 Services                   1      5,636 K
taskhost.exe                  2812 Services                   0      9,540 K
tasklist.exe                  1208 RDP-Tcp#0                  1      5,196 K
WmiPrvSE.exe                  1276 Services                   0      5,776 K
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server1 and svchost.exe

NEW QUESTION 187
A security analyst is reviewing malware files without running them. Which of the following analysis types is the security analyst using?

A. Dynamic
B. Sandbox

C. Static
D. Heuristic

Answer: C

Explanation:
Static analysis is the process of reviewing malware files without running them, by using tools such as hex editors, strings, and signature scanners. Static analysis can help extract basic information from malware files, such as file type, size, checksum, metadata, imports, exports, etc. Static analysis can also help identify known malware samples based on their signatures or hashes.

NEW QUESTION 189
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the most appropriate product category for this purpose?

A. SCAP
B. SOAR
C. UEBA
D. WAF

Answer: C

Explanation:
UEBA stands for User and Entity Behavior Analytics, which is a category of security products that use machine learning and statistical analysis to identify malicious actions by users or entities on a network. UEBA products can detect anomalous or suspicious behaviors that deviate from normal patterns or baselines, such as data exfiltration, privilege escalation, unauthorized access, insider threats, or compromised accounts. UEBA products can also provide alerts, reports, or recommendations for response actions based on the detected behaviors.

NEW QUESTION 192
A user receives a potentially malicious attachment that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would most likely indicate if the email is malicious?

A. sha256sum ~/Desktop/fi1e.pdf
B. /bin/;s -1 ~/Desktop/fi1e.pdf
C. strings ~/Desktop/fi1e.pdf | grep -i “<script”
D. cat < ~/Desktop/file.pdf | grep —i .exe

Answer: C

Explanation:
This command would most likely indicate if the email attachment is malicious, as it would display any JavaScript code embedded in the PDF file. JavaScript code can be used by attackers to execute malicious commands or scripts on the victim’s system when the PDF file is opened1. The strings command extracts the printable characters from a binary file, such as a PDF file, and the grep -i “<script” option searches for the presence of JavaScript code in a case-insensitive manner2.

NEW QUESTION 194
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?

A. SIEM
B. IDS
C. MFA
D. TLS

Answer: C

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user’s identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). MFA is the best control to help prevent credential stuffing attacks from being successful, because even if an attacker obtains a valid username and password from a breached site, they would still need another factor to access the target site. SIEM, IDS, and TLS are other security controls, but they are not as effective as MFA for preventing credential stuffing attacks.
Reference: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

NEW QUESTION 196
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 197
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 201
An organization is concerned about the proper handling of data and wants to implement measures to help safeguard customer data and the organization's proprietary information from exposure. Which of the following is the first step to improve awareness of overall privacy and protection?

A. Perform user acceptance testing.
B. Implement corporate policies.
C. Conduct biannual training.
D. Review data classification processes.

Answer: D

Explanation:
Data classification is the process of categorizing data based on its level of sensitivity, value, and risk. Data classification can help determine the appropriate level of protection and access control for each type of data.
Data classification processes should be reviewed regularly to ensure that they are aligned with the organization’s goals, policies, and standards. Data classification processes should also reflect the changing nature and value of data, as well as the evolving threats and regulations in the data environment.
Reviewing data classification processes can help improve awareness of overall privacy and protection by: ➢ Educating data owners and users about their roles and responsibilities in handling data.
➢ Establishing clear and consistent criteria for labeling and handling data.
➢ Identifying and prioritizing the most critical and sensitive data assets.
➢ Applying the appropriate security measures and controls for each data category.
➢ Reducing the risk of data loss, theft, or misuse.

NEW QUESTION 205
A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?

A. A static analysis to find libraries with flaws handling user inputs
B. A dynamic analysis using a dictionary to simulate user inputs
C. Reverse engineering to circumvent software protections
D. Fuzzing tools with polymorphic methods

Answer: D

Explanation:
Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities. Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex1. Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests2.
Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test. There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application1. Some examples of fuzzing tools are AFL, Peach, and [Sulley].
Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .
Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application’s functionality or security.

NEW QUESTION 207
A security analyst notices the following entry while reviewing the server togs OR 1=1' ADD USER attacker' PW 1337password' ---Which of the following events occurred?

A. CSRF
B. XSS
C. SQLi
D. RCE

Answer: C

Explanation:

SQLi stands for SQL injection, which is a type of attack that injects malicious SQL statements into a web application’s input fields or parameters. The attacker can use SQLi to execute unauthorized commands on the database server, such as adding a new user or retrieving sensitive data. The entry in the server logs shows an example of a SQLi attack that tries to add a new user named attacker with the password 1337password. CSRF, XSS, and RCE are other types of attacks, but they do not match the description of the entry in the server logs. Reference: https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 209
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. OpenIOC
C. CVSS
D. TAXlI

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.

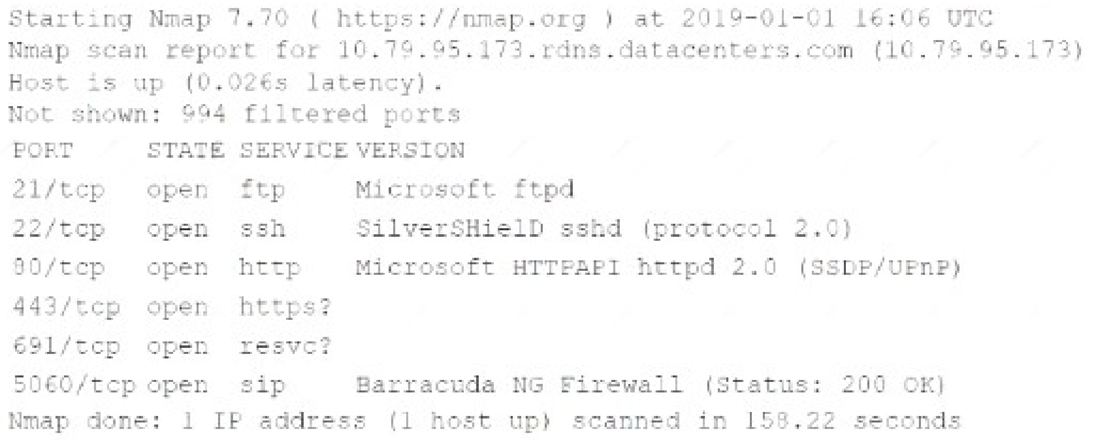
NEW QUESTION 214
A current, validated DLP solution Is now in place because of a previous data breach However, a new data breach has taken place The following symptoms were observed shorty after a recent sales meeting:
* Sensitive corporate documents appeared on the dark web.
* Unusually large packets of data were being sent out.
Which of the following is most likely occurring?

A. Documents are not tagged properly to restrict sharing.
B. An insider threat is exfiltration data.
C. The DLP solution is not configured for unsecured web traffic
D. File audits are not enabled on CASB.

Answer: B

Explanation:
This is most likely occurring based on the symptoms observed after a recent sales meeting. An insider threat is a person who has legitimate access to an organization’s network or data and uses it for malicious purposes, such as stealing, leaking, or sabotaging information. The symptoms suggest that someone from the sales team or someone who attended the meeting has copied sensitive corporate documents and uploaded them to the dark web using large data packets.

NEW QUESTION 218
An information security analyst is compiling data from a recent penetration test and reviews the following output:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
 PORT     STATE SERVICE VERSION
 21/tcp   open  ftp     Microsoft ftpd
 22/tcp   open  ssh     SilverSHielD sshd (protocol 2.0)
 80/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 443/tcp  open  https?
 691/tcp  open  resvc?
 5060/tcp open  sip     Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would most likely provide the needed information?

A. ping -t 10.79.95.173,rdns.datacenter.com
B. telnet 10.79.95.17.17 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79,,95,173

Answer: B

Explanation:
Telnet is a command-line tool that can be used to connect to a remote host on a specified port, and to send or receive data over that connection. Telnet can be used to obtain more information about the web-based services that are running on the target, by interacting with them or observing their responses. For example, telnet 10.79.95.173 443 would connect to the target on port 443, which is commonly used for HTTPS or SSL/TLS encrypted web traffic.

NEW QUESTION 223
A security analyst is supporting an embedded software team. Which of the following is the best recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation.
D. Perform a code review.

Answer: D

Explanation:
Performing a code review is the best recommendation to ensure proper error handling at runtime for an embedded software team. A code review is a process of examining and evaluating source code by one or more developers other than the original author. A code review can help to identify and fix any errors, bugs, vulnerabilities, or inefficiencies in the code before it is deployed or executed. A code review can also help to ensure that the code follows the best practices, standards, and guidelines for error handling at runtime .

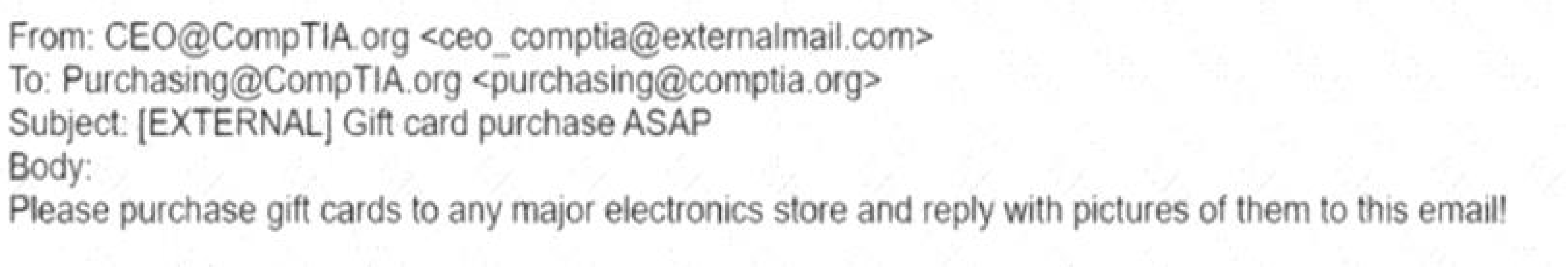
NEW QUESTION 224
A security analyst discovers suspicious activity going to a high-value corporate asset. After reviewing the traffic, the security analyst identifies that malware was successfully installed on a machine. Which of the following should be completed first?

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 225
An email analysis system notifies a security analyst that the following message was quarantined and requires further review.



From: CEO@CompTIA.org <ceo_comptia@externalmail.com>
To: Purchasing@CompTIA.org <purchasing@comptia.org>
Subject: [EXTERNAL] Gift card purchase ASAP
Body:
Please purchase gift cards to any major electronics store and reply with pictures of them to this email!

Which of the following actions should the security analyst take?

A. Release the email for delivery due to its importance.
B. Immediately contact a purchasing agent to expedite.
C. Delete the email and block the sender.
D. Purchase the gift cards and submit an expense report.

Answer: C

Explanation:
The email message that was quarantined and requires further review is an example of a phishing attempt that tries to trick the recipient into buying gift cards for a fake urgent request from a senior executive. The security analyst should delete the email and block the sender to prevent further attempts from reaching other users in the organization. Releasing the email for delivery, contacting a purchasing agent to expedite, or purchasing the gift cards and submitting an expense report are actions that would fall for the phishing attempt and result in financial loss or reputation damage for the organization. Reference:
https://www.csoonline.com/article/3444488/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent

NEW QUESTION 230
Which of the following activities is designed to handle a control failure that leads to a breach?

A. Risk assessment
B. Incident management
C. Root cause analysis
D. Vulnerability management

Answer: B

Explanation:
Incident management is a process that aims to handle a control failure that leads to a breach by restoring normal operations as quickly as possible and minimizing the impact and damage of the incident. Incident management involves activities such as identifying, analyzing, containing, eradicating, recovering, and learning from security incidents. Risk assessment, root cause analysis, and vulnerability management are other processes related to security management, but they are not designed to handle a control failure that leads to a breach. Reference:
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 233
An analyst needs to understand how an attacker compromised a server. Which of the following procedures will best deliver the information that is necessary to reconstruct the steps taken by the attacker?

A. Scan the affected system with an anti-malware tool and check for vulnerabilities with a vulnerability scanner.
B. Extract the server's system timeline, verifying hashes and network connections during a certain time frame.
C. Clone the entire system and deploy it in a network segment built for tests and investigations while monitoring the system during a certain time frame.
D. Clone the server's hard disk and extract all the binary files, comparing hash signatures with malware databases.

Answer: B

Explanation:
The correct answer is B. Extract the server’s system timeline, verifying hashes and network connections during a certain time frame. A system timeline is a chronological record of the events and activities that occurred on a system, such as file creation, modification, or deletion, process execution, registry changes, or network connections. A system timeline can help an analyst to understand how an attacker compromised a server by showing the sequence of actions and artifacts left by the attacker. An analyst can also verify the hashes of the files and processes involved in the compromise and compare them with known malware signatures or databases. Additionally, an analyst can check the network connections made by the server during the compromise and identify the source and destination IP addresses, ports, and protocols used by the attacker1.

NEW QUESTION 235
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 237
An organization has the following policy statements:
• AIl emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
•AM network activity will be logged and monitored.
• Confidential data will be tagged and tracked
• Confidential data must never be transmitted in an unencrypted form.
• Confidential data must never be stored on an unencrypted mobile device. Which of the following is the organization enforcing?

A. Acceptable use policy
B. Data privacy policy
C. Encryption policy
D. Data management, policy

Answer: B

Explanation:
Data privacy policy is the organization’s policy that defines how it collects, uses, stores, and shares personal data of its customers, employees, or other stakeholders. Data privacy policy also covers how the organization complies with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). The policy statements listed in the question are examples of data privacy policy provisions that aim to protect the confidentiality, integrity, and availability of personal data.

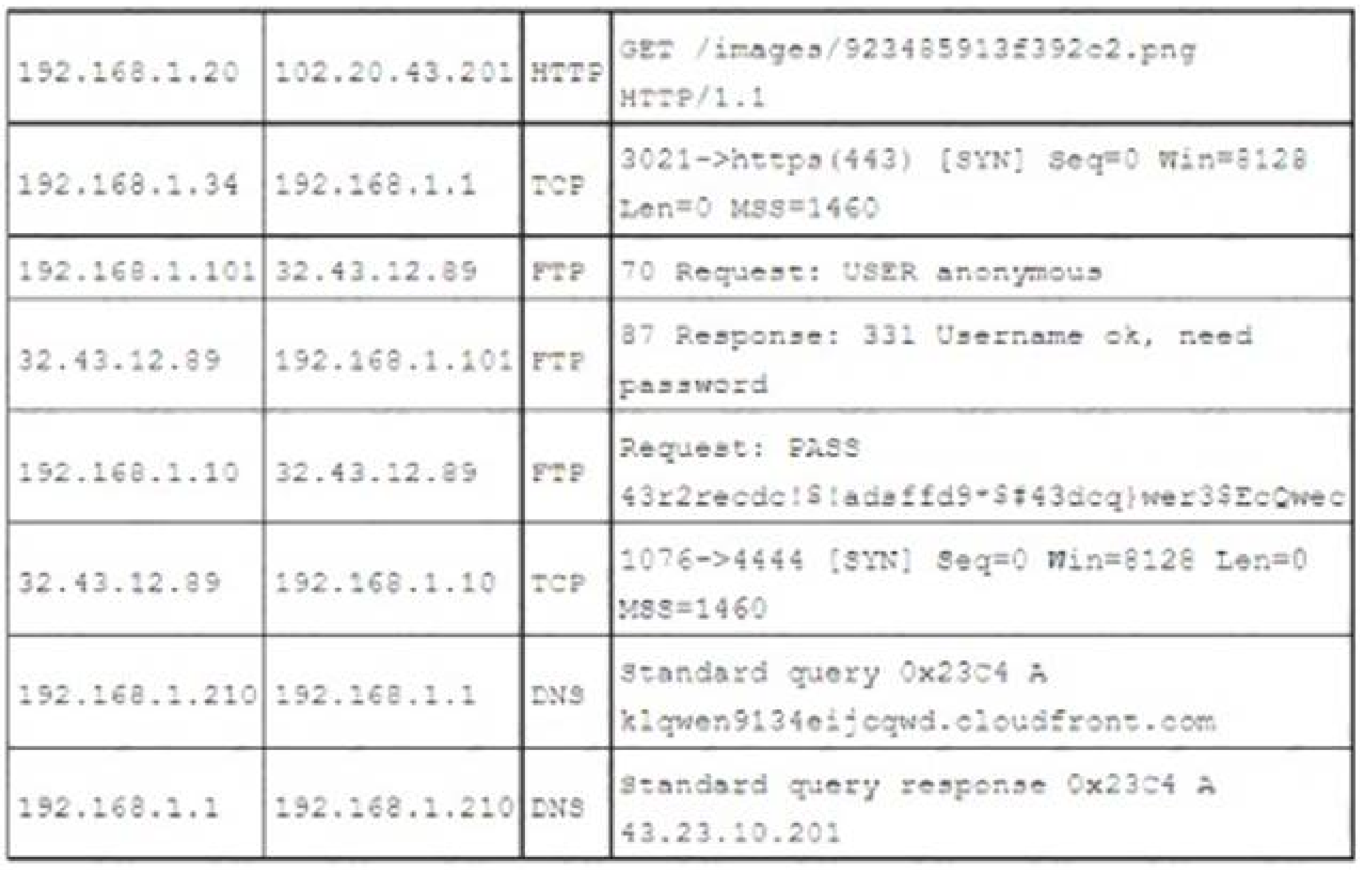
NEW QUESTION 240
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?

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 242
A security analyst reviews the following post-incident information to determine the origin and cause of a breach:



192.168.1.20	102.20.43.201	HTTP	GET /images/923485913f392c2.png HTTP/1.1
192.168.1.34	192.168.1.1	TCP	3021->https(443) [SYN] Seq=0 Win=8128 Len=0 MSS=1460
192.168.1.101	32.43.12.89	FTP	70 Request: USER anonymous
32.43.12.89	192.168.1.101	FTP	87 Response: 331 Username ok, need password
192.168.1.10	32.43.12.89	FTP	Request: PASS 43r2recdc!$!adsffd9~$#43dcq}wer3$EcQwec
32.43.12.89	192.168.1.10	TCP	1076->4444 [SYN] Seq=0 Win=8128 Len=0 MSS=1460
192.168.1.210	192.168.1.1	DNS	Standard query 0x23C4 A klqwen9134eijcqwd.cloudfront.com
192.168.1.1	192.168.1.210	DNS	Standard query response 0x23C4 A 43.23.10.201

Based on this information, which of the following should the analyst record in the incident report related to the breach? (Select two).

A. Forensic analysis Should be performed on 192.168, 1.10.
B. An on-path attack is impersonating the gateway.
C. IP address 43.23.10.201 should be blocked at the firewall.
D. Host 192.168.1.210 should be disconnected from the network.
E. The /images folder should be scanned with anti-malware.
F. A reverse shell was used.

Answer: CF

Explanation:

> F. A reverse shell was used: A reverse shell is a technique that allows a remote attacker to execute commands on a compromised system by opening a connection from the target to the attacker's machine. The image shows that the attacker used the netcat tool to create a reverse shell on host 192.168.1.210, which is running a web server on port 80. The attacker then used the reverse shell to access the /images folder and download a file named secret.jpg.

> C. IP address 43.23.10.201 should be blocked at the firewall: IP address 43.23.10.201 is the source of the attack, as shown by the netstat command output in the image. The attacker used this IP address to connect to host 192.168.1.210 on port 80 and exploit a vulnerability in the web server software. Blocking this IP address at the firewall would prevent further attacks from this source.

NEW QUESTION 245

A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

A. Input validation
B. Security regression testing
C. Application fuzzing
D. User acceptance testing
E. Stress testing

Answer: B

Explanation:

Detailed

Security regression testing is a type of testing that verifies that the security features and functionality of an application are not compromised or broken by any changes or updates in the code2. Security regression testing can help to ensure that the application follows industry best practices for secure coding and does not introduce any new vulnerabilities or weaknesses. Security regression testing can be performed manually or automatically using tools or scripts that check for common security flaws and compliance with security standards. Security regression testing can also help to validate the error-handling capabilities of an application by testing how it responds to different types of inputs and scenarios. Input validation (A) is a technique that checks whether the inputs to an application are valid and expected before processing them3. Input validation can help to prevent some types of security attacks, such as injection attacks or buffer overflows, but it is not a way to verify that an application follows industry best practices for secure
coding. Input validation is part of secure coding, not a way to test it. Application fuzzing © is a technique that tests an application by sending random or malformed inputs to it and observing its behavior4. Application fuzzing can help to discover some types of security vulnerabilities, such as memory leaks or crashes, but it is not a comprehensive way to verify that an application follows industry best practices for secure coding. Application fuzzing may not cover all possible inputs and scenarios and may not check for compliance with security standards. User acceptance testing (D) is a technique that tests an application by involving end users or customers in evaluating its functionality and usability. User acceptance testing can help to ensure that an application meets the user requirements and expectations, but it is not a reliable way to verify that an application follows industry best practices for secure coding. User acceptance testing may not focus on security aspects and may not detect subtle or hidden security flaws. Stress testing (E) is a technique that tests an application by subjecting it to high levels of load or demand. Stress testing can help to evaluate the performance and reliability of an application under extreme conditions, but it is not a relevant way to verify that an application follows industry best practices for secure coding. Stress testing does not check for security issues and may not reflect normal usage patterns.
References: 2: https://www.techopedia.com/definition/31686/resource-exhaustion 3: https://www.techopedia.com/definition/13493/penetration-testing 4: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl : https://www.techopedia.com/definition/24771/technical-controls : https://www.techopedia.com/definition/32088/vm-escape

NEW QUESTION 248

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 251
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 256
A security analyst is trying to track physical locations of threat actors via SIEM log information. However, correlating IP addresses with geolocation is taking a long time, so the analyst asks a security engineer to add geolocation to the SIEM tool. This is an example of using:

A. security orchestration, automation, and response.
B. continuous integration.
C. data enrichment.
D. threat feeds.

Answer: C

Explanation:
Data enrichment is a process that adds event and non-event contextual information to security event data in order to transform raw data into meaningful insights123. Geolocation is one example of contextual information that can be used to enrich security event data, such as IP addresses, and provide more information about the physical locations of threat actors. Data enrichment can help security analysts perform threat detection, threat hunting, and incident response more effectively and efficiently.

NEW QUESTION 257
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 258
Which of the following is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs?

A. Unifying and migrating all services in a single CSP

B. Executing an API hardening process on the CSPs' endpoints
C. Integrating the security benchmarks of the CSPs with a CASB
D. Deploying cloud instances using Nikto and OpenVAS

Answer: C

Explanation:
This is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs. CSP stands for cloud service provider, which is a company that offers cloud-based services such as infrastructure, platform, or software. CASB stands for cloud access security broker, which is a software or service that acts as a gateway between the company and the CSPs, and provides visibility, control, compliance, and threat protection for the cloud services.

Integrating the security benchmarks of the CSPs with a CASB means that the company can use a common set of standards and metrics to measure and compare the security posture and performance of different cloud service models, such as IaaS, PaaS, or SaaS. Security benchmarks are predefined criteria or best practices that define the minimum level of security required for a cloud service model. For example, some security benchmarks may include encryption, authentication, logging, auditing, patching, backup, etc. By integrating these benchmarks with a CASB, the company can monitor and enforce them across multiple CSPs, and identify any gaps or risks in their cloud security.

NEW QUESTION 262

......

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

100% Actual & Verified — Instant Download, Please Click
Order The CS0-002 Practice Test Here