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
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA
B. CAN bus
C. Modbus
D. IoT

Answer: B

Explanation:
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.
CAN bus stands for Controller Area Network bus, which is a communication protocol that allows different devices and components in a vehicle to communicate and exchange data. The vulnerability within the new fleet of vehicles is most likely targeting the CAN bus, because it could allow an attacker to manipulate or disrupt the operation of the vehicle. SCADA, Modbus, and IoT are other terms related to communication protocols or systems, but they are not specific to vehicles.
Reference: https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html

NEW QUESTION 3
During an audit, several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer. Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products. Which of the following would be the best way to locate this issue?

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

Answer: C

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

NEW QUESTION 4
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 5
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 6
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 7
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 8
Which of the following is the most effective approach to minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud?

A. Requiring security training certification before granting access to staff
B. Migrating all resources to a private cloud deployment
C. Restricting changes to the deployment of validated laC templates
D. Reducing laaS deployments by fostering serverless architectures

Answer: C

Explanation:
IaC stands for infrastructure as code, which is a practice of using code or configuration files to automate the provisioning and management of cloud resources. IaC templates can help ensure consistency, repeatability, and scalability of cloud deployments, as well as reduce human errors and misconfigurations. However, IaC templates need to be validated and tested before deployment, and any changes to the templates should be controlled and monitored. This can help minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud

NEW QUESTION 9
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 10
Which of the following is an advantage of continuous monitoring as a way to help protect an enterprise?

A. Continuous monitoring leverages open-source tools, thereby reducing cost to the organization.
B. Continuous monitoring responds to active Intrusions without requiring human assistance.
C. Continuous monitoring blocks malicious activity by connecting to real-lime threat feeds.

D. Continuous monitoring uses automation to identify threats and alerts in real time

Answer: D

Explanation:
Continuous monitoring uses automation to identify threats and alerts in real time. This is an advantage of continuous monitoring as a way to help protect an enterprise because it enables faster detection and response to security incidents, reduces the risk of human error, and improves the overall security posture and compliance of the organization.

NEW QUESTION 13
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

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

Answer: C

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

NEW QUESTION 17
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:
Creating a data minimization plan would be the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Data minimization is a principle that states that organizations should collect, store, process, and retain only the minimum amount of personal data that is necessary for their legitimate purposes. Data minimization can help reduce the risk of data breaches, data leaks, or data misuse by limiting the exposure and access to sensitive data. Data minimization can also help comply with data protection regulations, such as the General Data Protection Regulation (GDPR), that require organizations to justify their data collection and processing activities. Data minimization can be achieved by implementing various measures, such as deleting or anonymizing unnecessary data, applying retention policies, or using encryption or pseudonymization techniques.

NEW QUESTION 21
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 22
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.

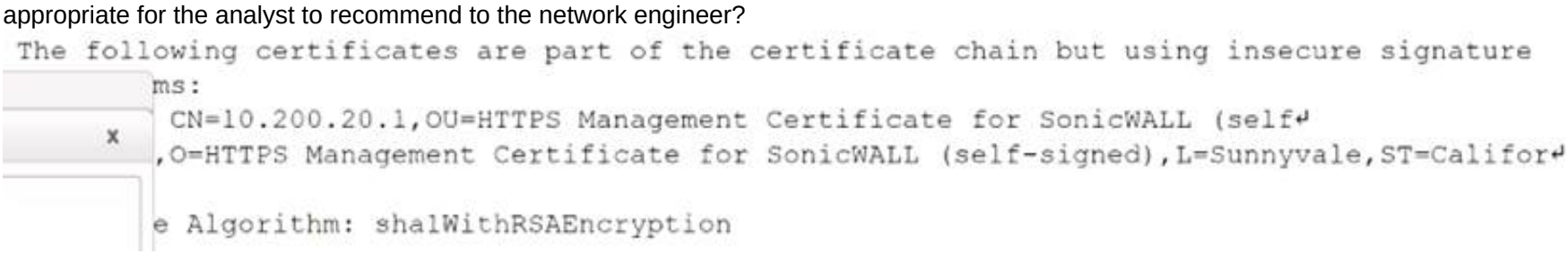
NEW QUESTION 27
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

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 31
While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report: this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?



A. Reconfigure the device to support only connections leveraging TLSv1.2.
B. Obtain a new self-signed certificate and select AES as the hashing algorithm.
C. Replace the existing certificate with a certificate that uses only MD5 for signing.
D. Use only signed certificates with cryptographically secure certificate sources.

Answer: A

Explanation:
The vulnerability assessment report shows that the device is using SSLv3, which is an outdated and insecure protocol for secure communication over a network. SSLv3 has several known vulnerabilities, such as POODLE, that allow attackers to decrypt or modify the encrypted data. To remediate this issue, the analyst should recommend reconfiguring the device to support only connections leveraging TLSv1.2, which is a newer and more secure protocol that provides stronger encryption, authentication, and integrity protection for the data transmitted over the network.

NEW QUESTION 34
During the onboarding process for a new vendor, a security analyst obtains a copy of the vendor's latest penetration test summary:

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

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

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

Answer: C

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

NEW QUESTION 38
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

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

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

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

Answer: B

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

NEW QUESTION 42
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

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

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

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

Answer: DF

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

NEW QUESTION 45
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 49
An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA
B. CAN bus
C. Modbus
D. loT

Answer: B

Explanation:
CAN bus (Controller Area Network) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer1. CAN bus is a message-based protocol, designed originally for multiplex electrical wiring within automobiles to save on copper, but it can also be used in many other contexts. CAN bus enables each device to send and receive data on a shared network, reducing the need for complex wiring and increasing reliability and performance. CAN bus is one of the five protocols used in the on-board diagnostics (OBD)-II vehicle diagnostics standard. A vulnerability within the new fleet of vehicles that the company recently purchased is most likely targeting CAN bus, as it is a common and critical communication system in modern vehicles. An attacker could exploit a vulnerability in CAN bus to compromise or manipulate various vehicle functions or systems, such as braking, steering, engine control, airbags, etc. SCADA (A) stands for Supervisory Control And Data Acquisition, which is a system that monitors and controls industrial processes or infrastructure2. SCADA is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. Modbus © is a serial communications protocol that connects industrial electronic devices3. Modbus is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. IoT (D) stands for Internet of Things, which is a network of physical objects that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. IoT is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl 3: https://www.techopedia.com/definition/31686/resource-exhaustion : https://www.techopedia.com/definition/13493/penetration-testing

NEW QUESTION 54
An organization is concerned about the security posture of vendors with access to its facilities and systems. The organization wants to implement a vendor review process to ensure \hi> policies implemented by vendors are in line with its own. Which of the following will provide the highest assurance of compliance?

A. An in-house red-team report
B. A vendor self-assessment report
C. An independent third-party audit report
D. Internal and external scans from an approved third-party vulnerability vendor

Answer: C

Explanation:
An independent third-party audit report can provide the highest assurance of compliance with the organization's policies by vendors, as it involves an objective and unbiased evaluation of the vendor's security posture and practices by an external auditor who follows established standards and criteria. An independent third-party audit report can help verify if the vendor meets the organization's requirements and expectations, as well as identify any gaps or weaknesses that need to be addressed.

NEW QUESTION 58
A security team has begun updating the risk management plan, incident response plan, and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?

A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review

Answer: C

Explanation:
According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, a tabletop exercise can be executed by internal managers to simulate and validate changes to the risk management plan, incident response plan, and system security plan. In a tabletop exercise, participants discuss and work through a simulated scenario, usually in a classroom or conference room setting, to evaluate their readiness and understanding of the proposed changes. This type of exercise can help to identify any potential issues or gaps in the proposed changes and can provide valuable insights for refining and improving the plans.

NEW QUESTION 62
An analyst is reviewing the following output as part of an incident:

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

Which of the Wowing is MOST likely happening?

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

D. Host 291.168.1.10 is performing firewall port knocking.

Answer: A

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

NEW QUESTION 67
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.
B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.
C. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.
D. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

Answer: B

Explanation:
Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1.

NEW QUESTION 70
Which of the following should a database administrator for an analytics firm implement to best protect PII from an insider threat?

A. Data deidentification
B. Data encryption
C. Data auditing
D. Data minimization

Answer: C

Explanation:
Data auditing is the most essential and effective method to protect PII from an insider threat. Data auditing is the process of monitoring and recording the activities and events related to data access and usage. Data
auditing can help detect and prevent any suspicious or anomalous behavior by an insider threat who tries to
access or manipulate PII.
Data auditing can provide several benefits for data protection, such as:

- It can provide accountability and transparency for data access and usage, which can deter potential insider threats from abusing their privileges or violating policies.
- It can provide evidence and traceability for data incidents, which can help investigate and respond to data breaches or leaks by insider threats.
- It can provide feedback and insights for data security improvement, which can help identify and address any gaps or weaknesses in data protection measures.

Data auditing can be done by using tools such as logs, alerts, reports, or dashboards. These tools can help security analysts track and analyze data activity and identify any patterns or anomalies that indicate a possible insider threat.

NEW QUESTION 71
A company needs to expand Its development group due to an influx of new feature requirements (rom Its customers. To do so quickly, the company is using Junior-level developers to fill in as needed. The company has found a number of vulnerabilities that have a direct correlation to the code contributed by the junior-level developers. Which of the following controls would best help to reduce the number of software vulnerabilities Introduced by this situation?

A. Requiring senior-level developers to review code written by junior-level developers
B. Hiring senior-level developers only
C. Allowing only senior-level developers to write code for new features
D. Using authorized source code repositories only

Answer: A

Explanation:
This control would best help to reduce the number of software vulnerabilities introduced by this situation because it ensures that code quality and security standards are met before deploying to production.
Senior-level developers can provide feedback, guidance, and corrections to junior-level developers and catch any errors or flaws in their code.

NEW QUESTION 72
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 74
While reviewing abnormal user activity, a security analyst notices a user has the following fileshare activities:

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

Which of the following should the analyst do first?

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

Answer: A

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

NEW QUESTION 79
Which of the following best explains why it is important for companies to implement both privacy and security policies?

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

Answer: D

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

NEW QUESTION 84
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 87
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 89
A security analyst scans the company's external IP range and receives the following results from one of the hosts:

Port:	Protocol:	State:
17	tcp/udp	close
21	udp	close
22	tcp	open
25	tcp	close
23	udp	close
53	udp	open
80	tcp/udp	close
139	tcp	close
389	tcp	close
443	tcp	close
3389	tcp	close
8080	tcp/udp	close
8443	tcp/udp	close

Which of the following best represents the security concern?

A. A remote communications port is exposed.
B. The FTP port should be using TCP only.
C. Microsoft RDP is accepting connections on TCP.
D. The company's DNS server is exposed to everyone.

Answer: C

Explanation:
The correct answer is C. Microsoft RDP is accepting connections on TCP. Microsoft RDP stands for Microsoft Remote Desktop Protocol, and it is a protocol that allows users to remotely access and control a Windows computer or server. RDP uses TCP port 3389 by default, and this port is open on the host according to the results. This indicates that the host is allowing RDP connections from anyone on the internet, which poses a security concern. An attacker could exploit vulnerabilities in RDP or use brute force attacks to gain unauthorized access to the host and compromise its data or resources1.
* A. A remote communications port is exposed is not correct. A remote communications port is a generic term for any port that allows remote access or communication with a host. There are many types of remote communications ports, such as SSH, Telnet, FTP, or RDP, and each one has its own security implications. The results do not specify which remote communications port is exposed, so this answer is too vague and inaccurate.
* B. The FTP port should be using TCP only is not correct. FTP stands for File Transfer Protocol, and it is a protocol that allows users to transfer files between hosts. FTP uses TCP ports 20 and 21 by default, and these ports are closed on the host according to the results. However, FTP can also use UDP ports 20 and 21 for data transfer in some cases, such as when using passive mode or extended passive mode2. Therefore, it is not true that FTP should be using TCP only, and this answer does not represent a security concern.
* D. The company’s DNS server is exposed to everyone is not correct. DNS stands for Domain Name System, and it is a system that translates domain names into IP addresses. DNS uses UDP port 53 by default, and this port is open on the host according to the results. This indicates that the host is providing DNS

services to anyone on the internet, which may or may not be a security concern depending on the configuration and purpose of the host. For example, if the host is a public DNS server that is intended to serve DNS queries from anyone, then this answer does not represent a security concern. However, if the host is a private DNS server that is meant to serve DNS queries only from authorized users or devices, then this answer could represent a security concern.
* 1: What Is Remote Desktop Protocol (RDP)? 2: FTP - File Transfer Protocol : [What Is Domain Name S (DNS)?]

NEW QUESTION 91
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 96
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 97
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

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

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

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

Answer: C

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

NEW QUESTION 101
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

A. The DNS configuration
B. Privileged accounts
C. The IDS rule set
D. The firewall ACL

Answer: C

Explanation:
The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or

malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not3. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

NEW QUESTION 105
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 107
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 108
A new government regulation requires that organizations only retain the minimum amount of data on a person to perform the organization's necessary activities. Which of the following techniques would help an organization comply with this new regulation?

A. Storing the highest-risk data in a separate and secured environment
B. Limiting access to data on a need-to-know basis
C. Deidentlfying a data subject throughout the organization's applications
D. Having a privacy expert peer review source code before deployment

Answer: C

Explanation:
Deidentifying a data subject means removing or obscuring any data that can be used to identify, locate, or contact an individual, such as names, addresses, phone numbers, email addresses, social security numbers, etc. Deidentifying a data subject throughout the organization’s applications can help comply with the new regulation that requires only retaining the minimum amount of data on a person to perform the organization’s necessary activities.

NEW QUESTION 109
A security analyst is reviewing a new Internet portal that will be used for corporate employees to obtain their pay statements. Corporate policy classifies pay statement information as confidential, and it must be protected by MFA. Which of the following would best fulfill the MFA requirement while keeping the portal accessible from the internet?

A. Obtaining home public IP addresses of corporate employees to implement source IP restrictions and requiring a username and password
B. Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN
C. Moving the internet portal server to a DMZ that is only accessible from the corporate VPN and requiring a username and password
D. Distributing a shared password that must be provided before the internet portal loads and requiring a username and password

Answer: B

Explanation:
Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN. This option provides the best MFA requirement because it uses two factors of authentication: something you have (smart card) and something you know (PIN). It also restricts access to the portal from a trusted source (corporate SSO internet endpoint).

NEW QUESTION 111

During a risk assessment, a senior manager inquires about what the cost would be if a unique occurrence would impact the availability of a critical service. The service generates $1 ,000 in revenue for the organization. The impact of the attack would affect 20% of the server's capacity to perform jobs. The organization expects that five out of twenty attacks would succeed during the year. Which of the following is the calculated single loss expectancy?

A. $200
B. $800
C. $5,000
D. $20,000

Answer: A

Explanation:
The single loss expectancy (SLE) is a measure of the monetary loss associated with a single occurrence of a risk. The SLE can be calculated by multiplying the asset value (AV) by the exposure factor (EF), which is the percentage of loss that the asset would suffer if the risk occurred. In this case, the asset value is the revenue generated by the service, which is $1,000. The exposure factor is the impact of the attack on the server's capacity, which is 20%. Therefore, the SLE is $1,000 x 0.2 = $2001.

NEW QUESTION 113
Which of the following factors would determine the regulations placed on data under data sovereignty laws?

A. What the company intends to do with the data it owns
B. The company's data security policy
C. The type of data the company stores
D. The data laws of the country in which the company is located

Answer: D

Explanation:
The data laws of the country in which the company is located would determine the regulations placed on data under data sovereignty laws. Data sovereignty laws are laws that govern how data is collected, stored, processed, and transferred within a country's jurisdiction. Data sovereignty laws can vary from country to country, depending on their legal system, political system, culture, and values. Data sovereignty laws can affect how companies handle their data, especially when they operate across borders or use cloud services. For example, some countries may have strict data protection or privacy laws that require companies to obtain consent from data subjects before collecting or processing their data. Some countries may also have data localization or data residency laws that require companies to store their data within the country's borders or limit cross-border data transfers.

NEW QUESTION 114
A security analyst needs to recommend a solution that will allow users at a company to access cloud-based SaaS services but also prevent them from uploading and exfiltrating data. Which of the following solutions should the security analyst recommend?

A. CASB
B. MFA
C. VPN
D. VPS
E. DLP

Answer: A

Explanation:
A cloud access security broker (CASB) is a solution that acts as a gatekeeper between users and cloud-based SaaS services. A CASB can enforce security policies, such as data loss prevention (DLP), encryption, authentication, or access control, to protect sensitive data from unauthorized access, upload, or exfiltration. A CASB can also provide visibility and monitoring of cloud usage and activity1.

NEW QUESTION 115
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 118
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

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

Answer: A

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

NEW QUESTION 119
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 122
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

Answer: B

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 .

NEW QUESTION 126
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

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

Answer: B

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

NEW QUESTION 131
An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the SDLC
process was overlooked?

A. Input validation
B. Planning

C. Implementation and integration
D. Operations and maintenance

Answer: B

Explanation:
The planning stage of the SDLC process is when the project scope, objectives, requirements, risks, and deliverables are defined and agreed upon by all stakeholders. This stage also involves creating a project plan that outlines the tasks, resources, schedule, budget, and communication channels for the project. The planning stage is crucial for ensuring that the project is aligned with the business goals and customer needs, and that the project team has a clear vision and direction for the development process. By overlooking this stage, the SOC staff did not receive contact details or escalation procedures to follow in case of a high-severity bug, which could have serious consequences for the security and functionality of the web application.

NEW QUESTION 133
A security is reviewing a vulnerability scan report and notes the following finding:

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

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

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

Answer: D

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

NEW QUESTION 135
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

A. Deterrent
B. Preventive
C. Compensating
D. Detective

Answer: C

Explanation:
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.
"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."
A compensating control is a control that reduces the risk of an existing or potential control weakness2
In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.

NEW QUESTION 139
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 140
A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:

Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEOVASLASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23zdcasdfAS	qscTRGvcaDFcaDCasDC23zdcasdfAS
lqkcjfc934cjcjvsad:cmaciwcfasd	lqkcjfc934cjcjvsad:cmaciwcfasd

Which of the following should the analyst report after viewing this Information?

A. A dynamic library that is needed by the executable a missing
B. Input can be crafted to trigger an Infection attack in the executable
C. The toot caused a buffer overflow in the executable's memory
D. The executable attempted to execute a malicious command

Answer: C

Explanation:
A buffer overflow is a type of attack that exploits a vulnerability in an application or program that does not properly check the size or boundaries of an input. A buffer overflow occurs when an attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations. This can result in unpredictable behavior, such as crashes, errors, data corruption, or execution of malicious code2
The tool that the analyst ran against the executable supplied an input that was too long for the buffer allocated by the executable. This caused a buffer overflow in the executable’s memory, as indicated by the error message “Segmentation fault (core dumped)”.

NEW QUESTION 143
A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to the senior management team? (Select TWO).

A. Probability
B. Adversary capability
C. Attack vector
D. Impact
E. Classification
F. Indicators of compromise

Answer: BD

Explanation:
According to the CompTIA CySA+ (CS0-002) best practices, the most useful information data points to provide to the security manager for communicating the risk factors to senior management are the impact and adversary capability. The impact refers to the potential consequences of a successful attack or exploitation of a vulnerability, such as data loss or system compromise. The adversary capability refers to the ability of an attacker to exploit a vulnerability, including their technical expertise and resources. Together, these data points help to provide a complete picture of the risk associated with a vulnerability, and allow senior management to make informed decisions regarding risk mitigation and remediation. The other data points, such as probability, attack vector, classification, and indicators of compromise, can also be valuable, but the impact and adversary capability are considered the most critical for prioritizing risk mitigation efforts.

NEW QUESTION 144
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 148
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

Answer: C

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. References: 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

NEW QUESTION 153
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 158
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 163
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 165
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.
B. The devices may have weak or known passwords.
C. The devices may cause a dramatic Increase in wireless network traffic.
D. The devices may utilize unsecure network protocols.
E. Multiple devices may interface with the functions of other loT devices.
F. The devices are not compatible with TLS 12.

Answer: BD

Explanation:
Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc. Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization’s network and data. Some of the reasons why consumer IoT devices should be avoided are:

- The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or

unauthorized access by attackers.

> The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

NEW QUESTION 168
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
```

Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.
C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.com.

Answer: C

Explanation:
The packet capture shows that the host sent a Client Hello message to utoftor.com on port 443. This message is part of the TLS (Transport Layer Security) handshake protocol, which is used to establish a secure connection between a client and a server1. The Client Hello message contains information such as the supported TLS version, cipher suites, and extensions that the client can use for the secure connection. The server is expected to respond with a Server Hello message that selects the parameters for the secure connection. However, the packet capture does not show any response from the server, which means that the host only attempted to make a secure connection to utoftor.com, but did not succeed. The host did not download (B) or reject (D) any application from utoftor.com.

NEW QUESTION 169
Which of the following solutions is the BEST method to prevent unauthorized use of an API?

A. HTTPS
B. Geofencing
C. Rate liming
D. Authentication

Answer: D

Explanation:
Authentication is a method of verifying a user's identity by requiring some piece 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). Authentication is the best method to prevent unauthorized use of an API, because it ensures that only legitimate users can access or use the API functions or data. HTTPS, geofencing, or rate limiting are other methods that can enhance the security or performance of an API, but they do not prevent unauthorized use of an API. Reference: https://www.redhat.com/en/topics/api/what-is-api-security

NEW QUESTION 170
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 174
A threat feed disclosed a list of files to be used as an loC 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 177
A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. The management team wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI
B. A hardware security module
C. eFUSE
D. Certificate signed updates

Answer: C

Explanation:
The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications. An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device authentication1.
* A. UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset2.
* B. A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset3.
* D. Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. 1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?

NEW QUESTION 182
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?

A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.

Answer: C

Explanation:
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.
The best way to remediate the vulnerability is to update to the secure hypervisor version. A hypervisor is a software that creates and manages virtual machines on a physical server. A hypervisor can be vulnerable to various attacks, such as privilege escalation, code injection, or denial-of-service. Updating to the secure hypervisor version can help fix any known bugs or flaws in the hypervisor software and prevent attackers from exploiting them. Updating to the secure hypervisor version can also provide additional security features or enhancements that can improve the protection of the virtual machines and their data.

NEW QUESTION 183
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 PII 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 PII.

NEW QUESTION 186
A security analyst is reviewing vulnerability scans from an organization's internet-facing web services. The following is from an output file called ssl-test_webapps.comptia.org:

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

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


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


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

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

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

Answer: A

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

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

The cipher suite in this line is weak because:

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

NEW QUESTION 191
Which of the following is a difference between SOAR and SCAP?

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

Answer: B

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

NEW QUESTION 194
A security analyst is reviewing the following Internet usage trend report:

Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?

A. User1
B. User 2
C. User 3
D. User 4

Answer: D

Explanation:
The Internet usage trend report shows that User 4 has an unusually high amount of data downloaded compared to other users. User 4 downloaded 2.5 GB of data in one day, while the average data downloaded by other users was around 0.2 GB. This could indicate that User 4 is engaged in some suspicious or malicious activity, such as downloading unauthorized or illegal content, exfiltrating sensitive data, or installing malware. Therefore, the security analyst should investigate User 4 further to determine the nature and source of the data downloaded.

NEW QUESTION 199
An incident response plan requires systems that contain critical data to be triaged first in the event of a compromise. Which of the following types of data would most likely be classified as critical?

A. Encrypted data
B. data
C. Masked data
D. Marketing data

Answer: B

Explanation:
PII stands for personally identifiable information, and it is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII data is considered critical because it can be used by attackers to commit identity theft, fraud, or other crimes. PII data is also subject to various laws and regulations that require organizations to protect it from unauthorized access, use, or disclosure1.

NEW QUESTION 202
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:

A. frameworks.
B. directors and officers.
C. incident response plans.
D. engineering rigor.

Answer: A

Explanation:
Ensuring that all areas of security have the proper controls is a primary reason why organizations use frameworks. Frameworks provide an organized structure for organizations to evaluate their security posture and implement the necessary security measures for their operations. Frameworks such as NIST, COBIT, and ISO 27001 provide guidance on how to develop, implement and monitor security policies, controls, and procedures for an organization. Additionally, frameworks provide a benchmark for organizations to measure their security posture against and create a roadmap for continued improvement.

NEW QUESTION 203
An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?

A. Requiring the use of the corporate VPN
B. Requiring the screen to be locked after five minutes of inactivity
C. Requiring the laptop to be locked in a cabinet when not in use
D. Requiring full disk encryption

Answer: D

Explanation:
Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NEW QUESTION 204
A security analyst needs to provide the development learn 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:
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.
VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

NEW QUESTION 209
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

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

Answer: C

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

NEW QUESTION 210
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 214

During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: C

Explanation:
Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege are part of a known threat modeling method called STRIDE. STRIDE is a mnemonic that stands for six categories of threats that can affect the security of a system or application. STRIDE was developed by Microsoft in 1999 and has been widely adopted as a threat modeling method by many organizations. STRIDE can help identify and prioritize potential threats based on their impact and likelihood1.

NEW QUESTION 215
A company's Chief Information Security Officer [CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the best technique to address the CISO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the files Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
F. Use Wireshark to scan all traffic to and from the director
G. Monitor the files for unauthorized changes.

Answer: B

Explanation:
Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes. This option is the best technique to ensure the integrity of the files and tie any changes to a specific user session. Hashing is a process that generates a unique value for a given input, and any modification to the input will result in a different hash value. By using SHA-256, which is a secure hashing algorithm, the analyst can compare the hash values of the files before and after each user session and detect any unauthorized changes.

NEW QUESTION 218
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 222
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:

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

Answer: C

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

NEW QUESTION 224
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 226
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 230
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 235
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 239
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 244
A technician working at company.com received the following email:

From: joe@gmail.com
To: technician@company.com
Subject: FW: Need help with my computer

Dear tech support,

Please contact me at +1-555-867-5309 as my computer was not fixed by the previous technician. My employee ID is 030234 and the computer serial # is A238482

---- Forward Message ----
From: joe@company.com
To: joe@gmail.com
Subject: FW: Need help with my computer

Dear joe, rebooting you computer should solve the issue.

After looking at the above communication, which of the following should the technician recommend to the security team to prevent exposure of sensitive information and reduce the risk of corporate data being stored on non-corporate assets?

A. Forwarding of corporate email should be disallowed by the company.
B. A VPN should be used to allow technicians to troubleshoot computer issues securely.
C. An email banner should be implemented to identify emails coming from external sources.
D. A rule should be placed on the DLP to flag employee IDs and serial numbers.

Answer: C

Explanation:
An email banner is a message that is added to the top or bottom of an email to provide some information or
warning to the recipient. An email banner should be implemented to identify emails coming from external sources to prevent exposure of sensitive information and reduce the risk of corporate data being stored on
non-corporate assets. An email banner can help employees recognize phishing or spoofing attempts and avoid clicking on malicious links or attachments. It can also remind employees not to share confidential information with external parties or forward corporate emails to personal accounts. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 13;
https://www.csoonline.com/article/3235970/what-is-spoofing-definition-and-how-to-prevent-it.html

NEW QUESTION 246
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 247
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 252
An intrusion detection analyst reported an inbound connection originating from an unknown IP address recorded on the VPN server for multiple internal hosts. During an investigation, a security analyst determines there were no identifiers associated with the hosts. Which of the following should the security analyst enforce to obtain the best information?

A. Update the organization's IP table.
B. Enable user access logging.
C. Shut down all VPN connections.
D. Create rules for the Active Directory.

Answer: B

Explanation:
User access logging (UAL) is a feature on Windows Server operating systems that records the details of
remote access and management activities performed by users on the server. UAL can provide information such as the user name, the source IP address, the destination host name, the protocol used, and the time and duration of the connection1. Enabling user access logging on the VPN server can help the security analyst to obtain the best information to identify and investigate the inbound connection originating from an unknown IP address.

NEW QUESTION 257
A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

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

Answer: B

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

NEW QUESTION 260
A financial organization has offices located globally. Per the organization’s policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

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

Answer: A

Explanation:
A mobile device wiping solution is a security feature that allows an organization to remotely erase or delete all data on a mobile device if it is lost or stolen2
A mobile device wiping solution can help protect the privacy of the data on a device and prevent unauthorized access or disclosure of sensitive information. A mobile device wiping solution can be implemented using built-in features of some mobile operating systems, third-party applications, or mobile device management (MDM) software.

NEW QUESTION 263
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 268
.....

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