(SY0-701)

CompTIA Security+ 2023

MYEXAM.FR

Total: **581 Questions**

Question: 1

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A.Hacktivist
B.Whistleblower
C.Organized crime
D.Unskilled attacker

Answer: C

Explanation:

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

While hacktivists, whistleblowers, and unskilled attackers might engage in disruptive activities, organized crime groups are the most likely to be employed by foreign governments for attacks on critical systems.
Here's a detailed justification:

1. **Resources and Expertise:** Organized crime syndicates often possess substantial financial resources and access to skilled individuals (including hackers) with the capabilities to conduct sophisticated attacks.

2. **Denial and Attribution:** Governments may seek to employ organized crime groups to maintain plausible deniability. The attack can be attributed to a criminal enterprise rather than the government itself, avoiding direct international repercussions.

3. **Specialized Skills:** Organized crime may already have experience in areas relevant to cyberattacks, such as money laundering, data theft, and extortion. This expertise can be readily adapted to state-sponsored cyber operations.

4. **Motivation:** Organized crime is often motivated by financial gain. While a government might provide direction and target selection, the criminal organization's primary incentive remains profit, which helps mask the state's involvement.

5. **Targeted Disruption:** Critical infrastructure attacks, such as those on power grids or communication networks, can destabilize a nation or disrupt its economy. Organized crime groups can be tasked with conducting these attacks on behalf of a foreign government to achieve specific geopolitical objectives.

6. **Cyber Mercenaries:** The concept of "cyber mercenaries" aligns with the use of organized crime. These groups offer their hacking skills to the highest bidder, and a foreign government may be the highest bidder for attacks that align with its strategic interests.

The other options are less likely:

Hacktivists: While politically motivated, they typically lack the resources and consistent direction needed for sustained attacks on critical infrastructure. Their actions are often more focused on raising awareness or making a statement.

Whistleblowers: Their primary goal is to expose wrongdoing, not to conduct destructive cyberattacks on behalf of foreign powers.

Unskilled attackers: Lack the technical skills and resources needed to attack critical systems.

Therefore, the combination of resources, skills, deniability, and motivation makes organized crime the most probable choice for a foreign government seeking to attack critical systems in another country.

MYEXAM.FR

Authoritative Links:

RAND Corporation:https://www.rand.org/ (Search for reports on cyber warfare, state-sponsored cyberattacks, and organized crime in cyberspace.)
Council on Foreign Relations:https://www.cfr.org/ (Look for articles and reports on cyber security and international relations.)
European Union Agency for Cybersecurity (ENISA):https://www.enisa.europa.eu/ (Search for reports on threat landscapes and cybercrime trends.)

Question: 2

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A.Key stretching
B.Data masking
C.Steganography
D.Salting

Answer: D

Explanation:

The correct answer is **D. Salting**.

Salting adds complexity to a password hashing process before the one-way hash function (like SHA-256 or bcrypt) is applied. A salt is a random string of characters added to each password before it is hashed. The purpose is to make rainbow table attacks and dictionary attacks much more difficult. Even if two users have the same password, the salt will be different, resulting in completely different hash values. Because the salt is prepended before the hashing algorithm is applied, it increases the pre-hashing complexity.

Let's examine why the other options are incorrect:

A. Key stretching: Key stretching techniques, like PBKDF2 or scrypt, repeatedly apply a hash function, usually after an initial hashing step, to make password cracking more computationally expensive. This isn't adding complexity before the one-way transformation, but rather iterating within it.

B. Data masking: Data masking obscures data, such as by replacing characters with asterisks or using data substitution. This helps protect sensitive data from unauthorized access, but it's unrelated to adding complexity to a hashing process.

C. Steganography: Steganography is the practice of concealing a message within another message or physical object. This is used to hide information, but it doesn't change or add complexity to the hashing process.

Therefore, salting is uniquely designed to add random data before applying the one-way hashing algorithm, rendering it the correct answer. It adds pre-hash complexity, which directly thwarts common password cracking methods.

Further Research:

OWASP on Salting: https://owasp.org/www-community/hashing
Key stretching vs salting: https://security.stackexchange.com/questions/3960/difference-between-key-stretching-and-salting

MYEXAM.FR

Question: 3

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

A.Brand impersonation

B.Pretexting

C.Typosquatting

D.Phishing

Answer: D

Explanation:

The correct answer is **D. Phishing**. Here's why:

Phishing is a type of social engineering attack where an attacker attempts to deceive a user into revealing sensitive information, such as usernames, passwords, credit card details, or other personal data, by disguising themselves as a trustworthy entity in an electronic communication.

In this scenario, the employee received an email seemingly from a legitimate payment website. This email prompted the employee to click a link and update their contact information. The crucial element is the deceptive nature of the email. The attacker is masquerading as the payment website, trying to trick the employee into thinking they are interacting with a legitimate source. Upon entering their login information, the user encounters a "page not found" error, which further supports the suspicion of a phishing attack. The attacker likely captured the login information entered before redirecting the user to a dead page or, potentially, a real page on the authentic site to avoid raising suspicion.

The other options are less likely:

A. Brand impersonation: While phishing often involves brand impersonation, brand impersonation in itself isn't the entire attack. It's the technique used within a phishing attempt.

B. Pretexting: Pretexting involves creating a fabricated scenario (the "pretext") to trick someone into divulging information or taking an action. While phishing can contain pretexting, the core of this attack is specifically about using a deceptive email/link.

C. Typosquatting: Typosquatting involves registering domain names that are slight misspellings of popular websites to trick users who misspell the address in their browser. This wasn't the attack vector in the scenario.

Therefore, the scenario aligns most directly with the definition of phishing because the attacker used a deceptive email (impersonating a payment website) with a malicious link to trick the employee into revealing sensitive information (login credentials). The "page not found" error is a common indicator of such attacks.

Authoritative Links:

NIST (National Institute of Standards and Technology) - Phishing:
https://csrc.nist.gov/glossary/term/phishing
SANS Institute - Understanding Phishing Attacks:https://www.sans.org/information-security/resources/glossary/phishing

Question: 4

An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

MYEXAM.FR

A.Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53

B.Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

C.Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53

D.Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Answer: D

Explanation:

Here's a detailed justification for why option D is the correct answer:

The objective is to restrict outbound DNS traffic, allowing only the device at IP address 10.50.10.25 to make DNS requests. Firewall Access Control Lists (ACLs) process traffic sequentially, so the order of rules is crucial.

Option D first **permits** traffic originating from 10.50.10.25 destined for any destination (0.0.0.0/0) on port 53 (DNS). The /32 signifies a single host (10.50.10.25). Then, the next rule **denies** all other outbound traffic (0.0.0.0/0 to 0.0.0.0/0) on port 53. The "deny any" rule acts as a catch-all, blocking DNS requests from any source IP other than 10.50.10.25. This is standard "permit specific, deny all others" logic.

Options A, B, and C are incorrect due to errors in the order of rules, source and destination IP configurations, or the logic of permit and deny statements. For example, Option A would permit all DNS traffic, then try to deny the traffic originating from 10.50.10.25, but the "permit any" rule will allow the traffic first. Similarly, options B and C have problems with either the permit rule or the deny rule configurations in reference to the question statement requirements.The correct logic of option D ensures that only authorized DNS traffic goes out while restricting any unwanted outbound DNS requests.

For further research, refer to these resources:

Cisco ACL Overview:https://www.cisco.com/c/en/us/support/docs/security/access-lists/13608-21.html
Understanding TCP/UDP Ports:https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/

Question: 5

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A.SSO
B.LEAP
C.MFA
D.PEAP

Answer: A

Explanation:

The correct answer is **A. SSO (Single Sign-On)**.

Here's why:

MYEXAM.FR

Single Sign-On (SSO) is an authentication method that enables users to access multiple applications and services with a single set of login credentials. In this scenario, the data administrator wants to leverage existing domain credentials (likely from Active Directory or a similar directory service) to authenticate users to a SaaS application. SSO is specifically designed to facilitate this.

Here's how it works: A user attempts to access the SaaS application. The application redirects the user to an Identity Provider (IdP). The IdP verifies the user's credentials against the existing domain directory. If successful, the IdP issues a security token (e.g., SAML, OAuth, or OIDC token) to the SaaS application. The SaaS application then trusts the IdP's assertion and grants the user access. This way, users don't need separate credentials for the SaaS application; they use their existing domain credentials. This reduces the number of passwords users need to remember and manage, improving security and user experience.

The other options are incorrect:

LEAP (Lightweight Extensible Authentication Protocol): LEAP is a proprietary wireless authentication protocol that is outdated and less secure than modern alternatives. It is not related to consolidating credentials for SaaS applications.

MFA (Multi-Factor Authentication): MFA adds an extra layer of security by requiring users to provide multiple verification factors. While valuable, MFA is in addition to an authentication method, not a replacement. MFA complements SSO, enhancing its security.

PEAP (Protected EAP): PEAP is another EAP protocol primarily used for wireless authentication, offering increased security over LEAP. Like LEAP, it's not the correct method to consolidate credentials for SaaS applications. It's more focused on securing wireless network access.

In summary, SSO is the direct and most appropriate solution for allowing users to access a SaaS application using their existing domain credentials, reducing the credential management burden.

Further Research:

NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management Cloud Security Alliance - SSO Explained

MYEXAM.FR

Question: 6

Which of the following scenarios describes a possible business email compromise attack?

A.An employee receives a gift card request in an email that has an executive’s name in the display field of the email.

B.Employees who open an email attachment receive messages demanding payment in order to access files.

C.A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.

D.An employee receives an email with a link to a phishing site that is designed to look like the company’s email portal.

Answer: C

Explanation:

The correct answer is C. Business Email Compromise (BEC) attacks specifically target employees with access to sensitive information or financial resources, aiming to deceive them into taking actions that benefit the attacker. Answer C directly illustrates this scenario. An attacker impersonating the HR director is attempting to obtain login credentials for a cloud administrator account. Gaining access to this account would grant the attacker significant control over the organization's cloud resources, allowing them to steal data, deploy malware, or disrupt services. This aligns perfectly with the intent and methodology of BEC attacks.

Option A, while a form of phishing, typically involves a simpler request and doesn't necessarily target sensitive access. Option B describes a ransomware attack, which is a distinct threat from BEC. Option D describes a phishing attack aiming to harvest credentials, but not necessarily targeting a cloud administrator.

Answer C is the strongest example of a BEC because it specifically targets high-level access (cloud administrator) by impersonating a person of authority (HR director). The attacker is seeking information (login credentials) that could lead to severe compromise of company assets in the cloud.

For further research, consult the following resources:

FBI - Business Email Compromise/Email Account Compromise:https://www.ic3.gov/complaint/default.aspx **CISA - Business Email Compromise (BEC):**https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-159a **Proofpoint - Business Email Compromise (BEC):**https://www.proofpoint.com/us/threat-reference/business-email-compromise-bec

Question: 7

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

A.Jump server

B.RADIUS

C.HSM

D.Load balancer

Answer: A

Explanation:

A jump server, also known as a bastion host, provides a secure, controlled point of access to internal network segments that are otherwise isolated or protected by firewalls. In this scenario, database administrators (DBAs) need access to database servers, but direct access from their workstations is prohibited. A jump server acts as an intermediary. The DBA would first connect securely to the jump server, then from the jump server, connect to the database servers within the secured segment. This configuration adds a layer of security by limiting the exposure of the database servers to direct connections from potentially compromised or less secured workstations. RADIUS is used for centralized authentication and authorization for network access, not for accessing internal servers. HSMs (Hardware Security Modules) are used for cryptographic key management, not for providing network access. Load balancers distribute network traffic across multiple servers to improve performance and availability, and are not designed for user access control. Therefore, a jump server is the most appropriate solution to enable DBAs to securely access the database servers without compromising the security of the network segment. It centralizes access control and monitoring, making auditing and security management much simpler. The use of multi-factor authentication on the jump server further strengthens the security posture.

For further reading:

NIST Special Publication 800-207 Zero Trust Architecture: Provides guidance on implementing a zero-trust architecture, where jump servers play a crucial role in segmenting access.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
AWS Documentation on Bastion Hosts: Describes the use of bastion hosts (jump servers) in the AWS cloud environment. https://docs.aws.amazon.com/quickstart/latest/linux/security.html

MYEXAM.FR

Question: 8

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

A.NGFW
B.WAF
C.TLS
D.SD-WAN

Answer: B

Explanation:

The correct answer is **B. WAF (Web Application Firewall)**. Here's why:

A buffer overflow exploit targets vulnerabilities within the application code itself, specifically how the application handles input data. An attacker sends more data than the application anticipates, causing it to overwrite memory regions, potentially allowing the attacker to execute arbitrary code.

A Web Application Firewall (WAF) is designed to inspect HTTP traffic (requests and responses) targeting web applications. It analyzes this traffic for malicious patterns, known attack signatures, and anomalies that indicate an attempt to exploit application vulnerabilities like buffer overflows. WAFs can be deployed in front of the web server to filter out malicious requests before they reach the application, thus preventing the exploit. They often use techniques like signature-based detection, anomaly detection, and positive security models (whitelisting allowed behaviors) to identify and block attacks.

While an NGFW (Next-Generation Firewall) provides broader network security, including intrusion detection and prevention, application control, and advanced threat protection, it primarily focuses on network-level security and might not be as effective at identifying and blocking application-specific attacks like buffer overflows. TLS provides encryption but doesn't protect against application-layer vulnerabilities. SD-WAN optimizes network performance and connectivity but is irrelevant to application-level attacks. WAFs are specifically designed for this type of web application vulnerability.

Therefore, deploying a WAF is the most effective measure to protect against future buffer overflow attacks targeting the organization's internet-facing website. It offers a focused defense at the application layer, mitigating the risk of exploiting coding flaws.

Further Research:

OWASP (Open Web Application Security Project):https://owasp.org/www-project-top-ten/ (See A03:2021 – Injection, which can lead to buffer overflows)
Cloudflare - What is a WAF?: https://www.cloudflare.com/learning/cloud-security/what-is-a-waf/

MYEXAM.FR

Question: 9

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A.Multifactor authentication
B.Permissions assignment
C.Access management
D.Password complexity

Answer: A

Explanation:

The correct answer is **A. Multifactor authentication (MFA)**.

Here's why: The scenario describes unauthorized access to user accounts, likely achieved through compromised credentials (passwords). Resetting passwords addresses the immediate issue, but doesn't prevent future password-based attacks.

MFA adds an extra layer of security beyond just a password. It requires users to provide two or more verification factors to gain access. These factors can include something they know (password), something they have (a code from a mobile app or hardware token), or something they are (biometrics). Even if an attacker obtains a user's password, they would still need to provide the additional factor to gain access.

Permissions assignment (B) is about granting appropriate access levels to users and resources, which doesn't directly prevent credential compromise. Access management (C) is a broader category encompassing policies and technologies for controlling access, but MFA is a specific and effective technique within access management for preventing unauthorized logins. Password complexity (D) helps make passwords harder to guess or crack, but it's not foolproof, and sophisticated attacks (e.g., phishing, credential stuffing) can still bypass complex passwords.

Therefore, MFA is the most effective solution to prevent future unauthorized logins from suspicious IP addresses because it requires additional verification beyond just a password, mitigating the risk of compromised credentials being exploited. By requiring a second factor, even if the initial password is stolen, the attacker will be unable to gain access.

Further Research:

NIST Guidelines on MFA: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
OWASP on MFA: https://owasp.org/www-project-top-ten/ (While not specifically dedicated to MFA, it highlights the importance of authentication in web application security).

MYEXAM.FR

Question: 10

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A.Typosquatting
B.Phishing
C.Impersonation
D.Vishing
E.Smishing
F.Misinformation

Answer: CE

Explanation:

The correct answer is C and E.

Here's why:

Impersonation (C): The text message is crafted to appear as if it originates from the payroll department. This act of pretending to be someone else to gain trust and extract information is a clear example of impersonation. The attacker is masquerading as a legitimate authority (the payroll department) to deceive the employee.

Smishing (E): Smishing is a type of phishing attack that occurs via SMS (Short Message Service), or text messaging. The scenario described involves a text message requesting credential verification, which is a classic tactic used in phishing attacks to steal sensitive information. Because the attack is delivered through text message, it is categorized as smishing.

Why the other options are incorrect:

Typosquatting (A): Typosquatting relies on users making typographical errors when entering a website address. This is not applicable to the scenario, which involves a text message.

Phishing (B): While the given scenario is technically phishing, smishing is the more specific type of phishing being used here. It is always better to select the most specific answer if available in these kinds of exams. **Vishing (D):** Vishing is phishing conducted over the phone (voice). The scenario involves a text message, not a phone call.

Misinformation (F): While the message itself could contain inaccurate information, the primary attack vector is impersonation through a fake request for credentials. The focus isn't on spreading false information generally, but on obtaining sensitive data through deception.

Supporting Information:

NIST defines Phishing in the context of Social Engineering, in the context of the scenario, Smishing is the specific type of Phishing occuring because it is SMS based.

NIST Definition:https://csrc.nist.gov/glossary/term/phishing

Smishing Definition - SANS Institute: Explains the process of carrying out SMishing, which is a type of phishing attack through SMS

https://www.sans.org/cyber-security-glossary/smishing/

Question: 11

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:

"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

A.Cancel current employee recognition gift cards.

B.Add a smishing exercise to the annual company training.

C.Issue a general email warning to the company.

D.Have the CEO change phone numbers.

E.Conduct a forensic investigation on the CEO's phone.

F.Implement mobile device management.

Answer: BC

Explanation:

The best responses to the CEO impersonation smishing attack are to issue a general email warning to the company (C) and add a smishing exercise to the annual company training (B).

Issuing a general email warning (C) promptly alerts all employees to the phishing scam, making them aware

MYEXAM.FR

that the CEO impersonation is happening. This allows individuals to be more vigilant and refrain from falling prey to the attacker if they receive similar messages. Early and widespread notification is crucial in mitigating the impact of phishing campaigns.

Adding a smishing exercise to the annual company training (B) proactively equips employees with the knowledge and skills to identify and avoid similar attacks in the future. The training can simulate real-world scenarios, enabling employees to develop critical thinking skills to recognize the red flags associated with smishing attacks. Employee education is the most effective defense against social engineering tactics.

Option A is not suitable, as canceling all employee recognition gift cards will penalize real award recipients. Option D may be necessary but not the best immediate response as phone numbers are easily spoofed. Option E is not necessarily relevant if the CEO did not send the message from their device. Option F is a valuable security measure but would require a more significant amount of time to implement than Options B and C.

Here are some resources:

NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations:https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (Focus on awareness and training controls)
SANS Institute:https://www.sans.org/ (Provides cybersecurity training and resources.)

Question: 12

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A.A thorough analysis of the supply chain

B.A legally enforceable corporate acquisition policy

C.A right to audit clause in vendor contracts and SOWs

D.An in-depth penetration test of all suppliers and vendors

Answer: A

Explanation:

The best approach to mitigate the risks of counterfeit hardware when certified hardware is mandated is **A. A thorough analysis of the supply chain.** This involves meticulously investigating each stage of the supply chain, from the manufacturer to the point of purchase. This deep dive aims to identify potential vulnerabilities and points where counterfeit components could be introduced.

A thorough supply chain analysis involves verifying the legitimacy and trustworthiness of each vendor, distributor, and sub-contractor involved. This includes checking certifications, conducting background checks, and potentially visiting facilities to ensure they meet security and quality standards. Focusing on the supply chain allows for proactive identification of potentially compromised links, preventing counterfeit hardware from entering the network infrastructure in the first place. While options C and D are valuable security measures, they are reactive, identifying issues after the hardware is already in use. Option B, a corporate acquisition policy, is irrelevant to addressing counterfeit hardware risks. By proactively vetting the supply chain, organizations can significantly reduce the risk of incorporating counterfeit hardware,
safeguarding the integrity and security of their networks. This proactive approach is the most effective way to ensure the use of genuine, certified hardware, aligning with compliance requirements and mitigating potential vulnerabilities.

Supply Chain Security Guidance:https://www.cisa.gov/supply-chain-security-guidance

MYEXAM.FR

Question: 13

Which of the following provides the details about the terms of a test with a third-party penetration tester?

A.Rules of engagement
B.Supply chain analysis
C.Right to audit clause
D.Due diligence

Answer: A

Explanation:

The correct answer is **A. Rules of Engagement**.

Rules of Engagement (RoE) are crucial when engaging a third-party penetration tester. They meticulously outline the boundaries, scope, and acceptable testing methods the tester can employ. This document dictates what systems are in scope, when the testing can occur (e.g., time windows), how intrusive the testing can be, and who to contact during the engagement. Essentially, the RoE acts as a contract defining the permitted actions of the penetration tester, preventing unintended consequences or legal ramifications from aggressive or out-of-scope activities. Without clearly defined RoE, the tester could potentially disrupt critical systems, violate legal agreements, or expose sensitive data during the penetration test. RoE also specify reporting requirements, detailing how vulnerabilities will be communicated and remediated. It protects both the organization hiring the tester and the tester themselves by setting clear expectations and limitations. Therefore, RoE precisely define the terms of engagement, making it the correct choice.

Supply chain analysis (B) assesses risks related to vendors and external dependencies, not the specifics of a penetration test. A right to audit clause (C) allows an organization to inspect a vendor's processes, and while it might be part of a broader agreement, it's not the primary document for defining pen test terms. Due diligence (D) is a general investigation performed before engaging a vendor; it does not specifically define the test parameters.

Relevant resource:

SANS Institute on Penetration Testing Agreements: https://www.sans.org/white-papers/39441/

MYEXAMER

Question: 14

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A.Active
B.Passive
C.Defensive
D.Offensive

Answer: A

Explanation:

The correct answer is **A. Active**.

Here's why: Active reconnaissance involves directly interacting with the target system to gather information. Port and service scanning, as described in the scenario, falls squarely within this definition. A penetration tester actively probes the target network by sending packets to various ports and analyzing the responses received. This interaction provides information about open ports, running services, operating systems, and potential vulnerabilities. These scans often use tools like Nmap, which actively transmits data. In contrast, passive reconnaissance gathers information without directly interacting with the target, such as analyzing publicly available data. Offensive and defensive are broader terms relating to the nature of the activity, but are not specifically types of reconaissance.

Active reconnaissance can potentially trigger intrusion detection systems (IDS) or other security measures, making it "noisier" and more easily detectable than passive reconnaissance. The Rules of Engagement document is thus essential as it outlines the permitted actions for a penetration tester during active reconnaisance.

Here are some resources you might find helpful:

OWASP Testing Guide: Information Gathering (Contains details on active and passive reconnaissance): https://owasp.org/www-project-web-security-testing-guide/latest/01-information-gathering/
NIST Special Publication 800-115: Guide to Security Testing (Provides an overview of different security testing techniques, including reconnaissance): https://csrc.nist.gov/publications/detail/sp/800-115/rev-1/final

Question: 15

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A.IRP
B.DRP
C.RPO
D.SDLC

Answer: B

Explanation:

The correct answer is DRP, which stands for Disaster Recovery Plan. A Disaster Recovery Plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster, whether natural or human-induced. For an organization to properly manage its restore process in the event of a system failure, a DRP is essential. It outlines the steps necessary to restore data, applications, and IT infrastructure to an operational state as quickly as possible, minimizing downtime and data loss.

Here's why the other options are less suitable:

IRP (Incident Response Plan): An IRP focuses on addressing security incidents and breaches, but it doesn't primarily cover the broader scope of system failures and restoration procedures. While an incident might lead to the need for restoration, the IRP doesn't provide a detailed recovery strategy.

RPO (Recovery Point Objective): RPO is a metric defining the maximum acceptable data loss in the event of a failure. It's crucial for determining backup strategies within a DRP, but it's not the plan itself. RPO informs how often backups should be performed, but doesn't describe the process of restoring from those backups.

SDLC (Software Development Life Cycle): SDLC is a process for planning, creating, testing, and deploying information systems. It has no direct relevance to system restoration after a failure.

In summary, a DRP is the comprehensive blueprint that organizations use to manage their restore process after a system failure. It defines roles, responsibilities, recovery strategies, and testing procedures, ensuring a coordinated and effective response to minimize business disruption. Without a robust DRP, organizations risk

MYEXAM.FR

prolonged downtime, significant data loss, and reputational damage.

Authoritative Links:

NIST Disaster Recovery:https://csrc.nist.gov/glossary/term/disaster_recovery
Ready.gov Disaster Recovery:https://www.ready.gov/business/implementation/IT

Question: 16

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A.Jailbreaking
B.Memory injection
C.Resource reuse
D.Side loading

Answer: D

Explanation:

The correct answer is D, Side loading. Here's why:

Side loading refers to the process of installing applications on a device without using the official app store or approved software repository of the manufacturer. This practice introduces several security vulnerabilities.

First and foremost, side-loaded applications bypass the security checks and vetting processes implemented by official stores like Google Play or Apple's App Store. These stores typically scan apps for malware, malicious code, and privacy violations before making them available to users. When an app is side-loaded, these checks are circumvented, significantly increasing the risk of installing a compromised application.

Secondly, side-loaded apps often lack the robust update mechanisms of apps installed from official stores. This means they may not receive critical security patches, leaving the device vulnerable to known exploits. Official stores provide a centralized system for delivering updates, ensuring that users have the latest security features and bug fixes.

Thirdly, the source of side-loaded apps is often untrustworthy. Users may download apps from unofficial websites, forums, or file-sharing services, which may distribute malware disguised as legitimate applications. It's difficult to verify the authenticity and integrity of these sources, making it easy for attackers to distribute malicious software.

Finally, side-loading can violate the device's security model, potentially granting the side-loaded application excessive permissions or access to sensitive data. Operating systems often enforce security policies that restrict the capabilities of applications installed from untrusted sources, but side-loading can bypass these restrictions.

Jailbreaking (A) removes software restrictions imposed by the manufacturer and typically isn't directly related to software vulnerabilities. Memory injection (B) is a technique where malicious code is inserted into the memory of a running process, which isn't inherently tied to the method of software installation. Resource reuse (C) refers to the re-use of a previous resource and not a software installation vulnerability.

In essence, side-loading undermines the security measures put in place by manufacturers to protect users from malware and other security threats.

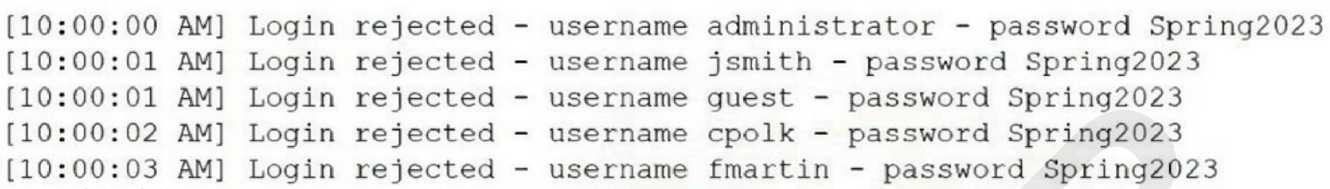
Reference:

MYEXAM.FR

Sideloading apps and why it's potentially dangerous: https://www.androidauthority.com/sideloading-885007/ What is Sideloading?: https://www.kaspersky.com/resource-center/definitions/what-is-sideloading

Question: 17

A security analyst is reviewing the following logs:



```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A.Password spraying

B.Account forgery

C.Pass-the-hash

D.Brute-force

Answer: A

Explanation:

Password spraying is a type of brute-force attack used to gain unauthorized access to user accounts by systematically attempting a small number of commonly used passwords against many user accounts. Unlike traditional brute-force attacks, which attempt many different passwords against a single user account, password spraying involves trying a few commonly used passwords against a large number of accounts.

Question: 18

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

A.Secured zones

B.Subject role

C.Adaptive identity

D.Threat scope reduction

Answer: A

Explanation:

The correct answer is **A. Secured zones**.

Here's why: Zero Trust, particularly within the data plane, focuses on protecting data at rest and in transit. The data plane is where the actual data resides and moves. Secured zones, implemented through microsegmentation or network segmentation, create isolated areas within the network. This limits the blast radius of a potential breach, a core tenet of Zero Trust. By segmenting the network and applying strict access controls between zones, you minimize lateral movement. Every request for data access requires authentication and authorization, irrespective of its origin within the internal network.

"Subject role" (B) relates to role-based access control, which is a component of Zero Trust but is more pertinent to identity and access management (IAM) outside of the immediate data plane. While role definitions

MYEXAM.FR

are helpful to reduce the attack surface, it isn't the most important for evaluating the data plane's Zero Trust implementation. "Adaptive identity" (C) involves dynamically adjusting access privileges based on user behavior and risk assessment, enhancing identity verification but focuses less directly on securing the data itself at rest and transit. "Threat scope reduction" (D) is a general security principle. Secured zones are a specific technique for achieving this within the data plane.

Secured zones are a fundamental technique for implementing Zero Trust within the data plane because they enforce the principle of least privilege and assume that any part of the network could be compromised. This necessitates granular access controls and the isolation of data within specific zones. The principle of least privilege is the concept that a user or process should have only the access to resources that are absolutely necessary to perform their job.

Therefore, while other options touch upon aspects of Zero Trust, secured zones are most directly related to protecting data within the data plane under a Zero Trust model.

For further reading:

NIST Special Publication 800-207 (Zero Trust Architecture):
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
Cloud Security Alliance (CSA) Guidance:https://cloudsecurityalliance.org/ (Search for Zero Trust related resources)

Question: 19

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A.RDP server
B.Jump server
C.Proxy server
D.Hypervisor

Answer: B

Explanation:

The correct answer is **B. Jump server**.

A jump server, also known as a bastion host, acts as an intermediary between external networks and internal resources. This configuration significantly enhances security by funneling all remote access through a single, hardened point. Instead of directly exposing internal servers to the internet, users first connect to the jump server, which then facilitates access to the targeted internal system.

This architecture minimizes the attack surface, as attackers would need to compromise the jump server before gaining access to anything else. Jump servers are typically hardened with strict access controls, multi-factor authentication, and regular security audits. They are often placed in a demilitarized zone (DMZ), further isolating internal networks. The jump server also provides a central point for logging and auditing all remote access activity, improving security monitoring and incident response capabilities.

Option A, RDP server, is incorrect because it directly exposes internal servers to RDP connections, increasing the attack surface. Option C, a proxy server, is primarily used for web traffic filtering and caching, not for securing remote access to internal resources. Option D, a hypervisor, is a virtualization platform and not directly involved in controlling remote access in the manner needed for increased security. A jump server is specifically designed for this purpose.https://www.trendmicro.com/vinfo/us/security-news/cybercrime-and-digital-threats/what-is-a-jump-server-and-how-does-it-help-secure-a-

MYEXAM.FR

networkhttps://www.fortinet.com/resources/cyberglossary/jump-server

Question: 20

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A.encryption=off

B.http://

C.www.*.com

D.:443

Answer: B

Explanation:

The correct answer is **B. http://**. Here's why:

A web filter analyzing URLs to block non-encrypted traffic aims to prevent users from accessing websites using the unencrypted HTTP protocol.

Why "http://" is the best choice:

Direct Protocol Identification: The string "http://" is the definitive identifier for the HTTP protocol in a URL. Detecting this string explicitly signals a non-encrypted connection.

Precise Targeting: Filtering for "http://" directly targets the unencrypted protocol without relying on potentially unreliable cues like the presence of specific ports or keywords.

Why other options are less suitable:

A. encryption=off: While some websites might use query parameters like "encryption=off" (or something similar), this isn't a universal standard. Relying on such parameters would only block a small subset of unencrypted websites. Most sites simply lack encryption and don't explicitly signal its absence.

C. www.*.com: This pattern is too broad. It would block access to numerous websites regardless of their encryption status. Many secure (HTTPS) websites use this pattern.

D. :443: Port 443 is the standard port for HTTPS (encrypted) traffic, not HTTP. Blocking this port would hinder access to secure websites, the opposite of the goal.

Therefore, the search string "http://" is the most effective and direct method for a web filter to identify and block access to non-encrypted websites. It directly targets the protocol indicator, ensuring that only HTTP sites are blocked while allowing HTTPS sites to function normally.**Authoritative Links for further research:**

HTTP vs HTTPS:https://www.cloudflare.com/learning/ssl/http-vs-https/
URL Structure:https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL **Web filtering:**https://www.techtarget.com/searchsecurity/definition/Web-filtering

MYEXAM.FR

Question: 21

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A.access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32

B.access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

C.access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D.access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation:

The correct answer is B because it accurately reflects the logic needed to block inbound traffic from a specific IP address. Let's break it down:

The objective is to deny access from the malicious IP (10.1.4.9) to our organization's network. Therefore, we need a "deny" rule where the source is the malicious IP and the destination is anything on our network.

"access-list inbound deny ip": This part sets up an access control list (ACL) for inbound traffic and specifies that this rule is designed to deny traffic. The "ip" parameter indicates that this rule applies to IP traffic.

"source 10.1.4.9/32": This specifies the source IP address that will be blocked. /32 is a CIDR notation that means only traffic originating exactly from 10.1.4.9 will be blocked (as opposed to a range of IPs). This is important as we only want to block the malicious address, not a whole subnet.

"destination 0.0.0.0/0": This specifies the destination IP address. 0.0.0.0/0 represents any destination IP address. In this context, it means any IP address on our network. Therefore, the rule blocks traffic from 10.1.4.9 to any IP address within our organization.

Options A, C, and D are incorrect for the following reasons:

A: This rule attempts to block traffic to the malicious IP, not from it. The source is set to 0.0.0.0/0 which signifies "any" and the destination is 10.1.4.9/32.

C: This rule is a "permit" rule, meaning it would allow traffic from the specified IP, which is the opposite of what we want.

D: Similar to A, this is a "permit" rule aimed at allowing traffic to the malicious IP.

In summary, the correct rule (B) effectively prevents the malicious IP address from initiating any connection to any resource within the organization's network. This implements a standard security practice of blacklisting known malicious sources.

Further reading:

Cisco Access Control Lists (ACLs):https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/acl/configuration/15-sy/sec-acl-15-sy-book.html (While this example might be Cisco-centric, the concept of ACLs and their source/destination logic is widely applicable.)

CIDR Notation:https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

MYEXAM.FR

Question: 22

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

A.Implementing a bastion host

B.Deploying a perimeter network

C.Installing a WAF

D.Utilizing single sign-on

Answer: A

Explanation:

The correct answer is **A. Implementing a bastion host**.

A bastion host, also known as a jump server, provides a hardened and secured gateway to access internal resources. It resides within the security boundary (e.g., a network or VPC) and is the only machine allowed to accept connections from external sources for administrative purposes. This significantly reduces the attack surface by limiting the number of entry points into the internal network. Administrators connect to the bastion host first, then from the bastion host, they connect to other internal resources using SSH, RDP, or other administrative protocols.

Option B, deploying a perimeter network (DMZ), is primarily for hosting publicly accessible services and doesn't inherently restrict administrative access in the most secure way. While a DMZ adds a layer of security, it doesn't inherently control or limit the traffic permitted for administrators accessing internal systems.

Option C, installing a WAF (Web Application Firewall), protects web applications from common attacks like SQL injection and cross-site scripting. It's not directly related to securing administrative access to internal resources, but rather focuses on protecting web applications.

Option D, utilizing single sign-on (SSO), simplifies authentication and authorization across multiple applications but does not inherently minimize the traffic allowed through the security boundary. SSO streamlines user access but doesn't offer the same level of network isolation or access control as a bastion host.

Bastion hosts are frequently employed in cloud environments to facilitate secure administrative access to virtual machines, databases, and other internal resources. By restricting direct access from the outside, they greatly reduce the risk of compromise. The bastion host can be further hardened with multi-factor authentication, intrusion detection systems, and regular security patching.

Authoritative Links:

Microsoft Azure Bastion:https://learn.microsoft.com/en-us/azure/bastion/bastion-overview
AWS Bastion Hosts:https://aws.amazon.com/quickstart/architecture/linux-bastion/

MYEXAM.FR

Question: 23

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

A.Application
B.IPS/IDS
C.Network
D.Endpoint

Answer: D

Explanation:

The correct answer is **D. Endpoint**. Here's why:

The scenario requires obtaining detailed information about an executable running on an employee's laptop to investigate potential malicious activity. An endpoint log, typically collected by Endpoint Detection and

Response (EDR) or Host-based Intrusion Detection Systems (HIDS), provides precisely this kind of data.

Endpoint logs capture process execution details, including the executable's name, path, hash values (like MD5 or SHA256), parent processes, command-line arguments, network connections initiated by the process, and modifications to the file system or registry. This granular data is crucial for determining if an executable is malicious.

Application logs (A) record events specific to applications running on a system, such as errors, warnings, or informational messages. They might not contain the specific executable details needed for this investigation. IPS/IDS logs (B) focus on detecting and preventing malicious network activity, often at the network perimeter, and may not provide in-depth insights into processes running on individual endpoints. Network logs (C) capture network traffic data, such as source and destination IP addresses, ports, and protocols. While helpful for identifying suspicious communication patterns, they lack the detailed executable information needed to assess if a process is malicious.

Endpoint logs are specifically designed to monitor and record activities occurring on individual systems, making them the most appropriate source for the requested data. They allow security analysts to deeply examine the behavior of executables and processes, aiding in malware analysis and incident response. Therefore, consulting the endpoint logs is the most direct and effective way to gather the required data about the potentially malicious executable running on the employee's laptop.

For further research, consider exploring resources on EDR and HIDS solutions:

CrowdStrike: What is EDR?https://www.crowdstrike.com/cybersecurity-101/endpoint-detection-response-edr/
Qualys: Host Intrusion Detection System (HIDS)https://www.qualys.com/apps/host-intrusion-detection-system-hids/

Question: 24

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

A.Digital forensics
B.E-discovery
C.Incident response
D.Threat hunting

Answer: D

Explanation:

The correct answer is **D. Threat hunting**. Here's why:

Threat hunting is a proactive security activity focused on discovering malicious activities that have bypassed existing security measures. Since the SIEM alerts are not yet configured to detect the new tactic, traditional reactive security mechanisms will be ineffective. Threat hunting involves actively searching for anomalies and suspicious patterns within the network and systems, leveraging threat intelligence and security expertise.

Digital forensics (A) is primarily concerned with investigating security incidents after they have occurred to determine the cause and scope of the breach, which is not the immediate need here. E-discovery (B) is a legal process related to identifying and collecting electronic evidence, and is irrelevant to proactive identification of malicious activity. Incident response (C) is a structured approach to handling security incidents after they

MYEXAM.FR

have been detected, and while valuable, is not the initial step when seeking out unknown threats.

Threat hunting aligns directly with the situation. The security analyst needs to proactively search for evidence of the new malicious tactic, analyze network traffic, system logs, and endpoint data to identify potentially compromised systems or accounts before a full-blown incident occurs. This is the essence of threat hunting. The aim is to find threats that automated systems are currently missing, therefore filling the gap until SIEM rules can be updated.

Further research:

SANS Institute on Threat Hunting: https://www.sans.org/cyber-security/threat-hunting/
NIST Special Publication 800-207 Zero Trust Architecture:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (While not directly about Threat Hunting, Zero Trust principles drive the need for continuous monitoring and threat hunting activities.)

Question: 25

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

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

Answer: B

Explanation:

The correct answer is **B. Transfer**. Here's why:

Risk transfer involves shifting the burden of financial loss associated with a risk to a third party. Purchasing cyber insurance is a prime example of risk transfer. The company is essentially paying a premium to the insurance provider, who in turn agrees to cover certain financial losses that might arise from cybersecurity incidents, such as data breaches, ransomware attacks, or denial-of-service attacks.

Acceptance means acknowledging a risk and deciding to take no action. This is not what the company is doing by purchasing insurance.

Mitigation involves taking steps to reduce the likelihood or impact of a risk. While the company may also implement security controls, purchasing insurance specifically addresses the financial impact, not the risk itself.

Avoidance means eliminating the activity or condition that gives rise to the risk. Cyber insurance doesn't eliminate cybersecurity risks; it merely helps manage the consequences.

By transferring the financial risk to the insurance company, the company reduces its potential liability in the event of a cybersecurity incident that results in financial loss. Insurance policies often cover expenses such as legal fees, notification costs, credit monitoring for affected individuals, and even business interruption losses. This proactive measure, outlined in the company's risk register, demonstrates a deliberate decision to transfer a portion of its financial exposure to another entity. Therefore, the correct risk management strategy being employed is **transfer**.

Here are some authoritative resources for further research:

NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments:

MYEXAM.FR

https://csrc.nist.gov/publications/detail/sp/800-30/r1/final (Provides guidance on risk management processes, including risk transfer.)

SANS Institute:https://www.sans.org/ (Offers various courses and resources on cybersecurity, including risk management.)

Cybersecurity & Infrastructure Security Agency (CISA):https://www.cisa.gov/ (Provides information and resources on cybersecurity risk management.)

Question: 26

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

A.Partition
B.Asymmetric
C.Full disk
D.Database

Answer: C

Explanation:

The correct answer is **C. Full disk encryption**.

Full disk encryption (FDE) is the most appropriate technique for protecting all data on employee laptops because it encrypts the entire hard drive, including the operating system, applications, and user data. This ensures that even if a laptop is lost or stolen, the data remains inaccessible to unauthorized individuals without the proper decryption key or passphrase.

Partition encryption (A) only encrypts a specific section of the disk, leaving other areas unprotected. Asymmetric encryption (B) is primarily used for secure communication and key exchange, not for encrypting large amounts of data at rest. Database encryption (D) specifically targets databases and doesn't offer comprehensive protection for all the data on a laptop.

FDE protects against various threats, including data breaches resulting from lost or stolen devices, unauthorized access by malicious software, and data recovery attempts after a device is decommissioned. Solutions like BitLocker (Windows) and FileVault (macOS) provide built-in full disk encryption capabilities.

In a corporate environment, managing FDE involves implementing policies for key management, password strength, and recovery procedures. This usually involves central management systems that can remotely enforce encryption policies, manage encryption keys, and assist with data recovery if needed.

The need for compliance with data privacy regulations such as GDPR, HIPAA, and CCPA often mandates the implementation of FDE as a crucial security control. Organizations may also be required to implement FDE to comply with industry best practices and security standards.

Further reading:

NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices:
https://csrc.nist.gov/publications/detail/sp/800-111/final
Microsoft BitLocker Overview: https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
Apple FileVault Overview: https://support.apple.com/en-us/HT204837

MYEXAM.FR

Question: 27

Which of the following security control types does an acceptable use policy best represent?

A.Detective

B.Compensating

C.Corrective

D.Preventive

Answer: D

Explanation:

The best answer is D, Preventive. An acceptable use policy (AUP) outlines the rules and guidelines for using an organization's resources, including systems, networks, and data. It aims to prevent inappropriate or unauthorized activities before they occur. By clearly defining acceptable and unacceptable behaviors, an AUP educates users about security expectations and discourages them from engaging in actions that could compromise security. This proactive approach is the core of preventive security controls. Detective controls, on the other hand, identify security incidents after they have happened. Compensating controls are implemented as alternatives when primary controls are infeasible or ineffective. Corrective controls are employed to remediate the effects of a security incident. While an AUP might contribute to detecting violations or triggering corrective actions after the fact, its primary function is to prevent those violations in the first place through education and policy enforcement. The proactive stance makes it definitively a preventive control. The AUP acts as the first line of defense.

For further reading and understanding of Security Controls:

NIST Special Publication 800-53:https://csrc.nist.gov/publications/detail/sp/800-53/r5/final (Describes security and privacy controls for information systems and organizations)
SANS Institute:https://www.sans.org/ (Offers courses and resources on security controls and best practices)

MYEXAM.FR

Question: 28

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

A.Hardening

B.Employee monitoring

C.Configuration enforcement

D.Least privilege

Answer: D

Explanation:

The IT manager is implementing the principle of least privilege. Least privilege is a security concept where users are given the minimum level of access necessary to perform their job functions. In this scenario, the help desk staff only needs to access the basic functionalities of the help desk software to assist users. Granting them administrative access would violate the principle of least privilege, as it provides them with capabilities beyond what is required for their roles. Only the IT manager and help desk lead, who likely require administrative access for configuration, maintenance, and reporting, are granted those elevated permissions.

Configuration enforcement (option C) is related but not the primary focus. While limiting access can contribute to configuration security, the core action here directly addresses access rights. Employee monitoring (option B) is not relevant as the action is about access control, not observation. Hardening (option A) refers to reducing a system's attack surface and is a broader term than simply restricting access. The scenario directly reflects the principle of only granting necessary permissions. By restricting administrative access to only those who require it, the IT manager minimizes the potential for accidental or malicious misuse of the help desk software. This reduces the overall risk to the organization's data and systems.

For further research, refer to these resources:

NIST (National Institute of Standards and Technology):https://csrc.nist.gov/glossary/term/least_privilege
OWASP (Open Web Application Security Project):https://owasp.org/www-project-top-ten/ (While not directly about least privilege, it provides context on vulnerabilities mitigated by such practices)

Question: 29

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A.Risk tolerance
B.Risk transfer
C.Risk register
D.Risk analysis

Answer: C

Explanation:

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

A risk register is a crucial document in risk management, specifically designed to systematically record and track identified risks, their potential impact, probability, and the planned response strategies. It serves as a central repository for all information related to risk management within an organization or project. The register typically includes a description of each risk, the likelihood of it occurring, the potential impact if it does occur, the assigned owner (responsible party) for managing the risk, and the defined thresholds that trigger specific actions or escalations. It may also contain mitigation strategies and contingency plans. The risk register aids in communication among stakeholders, facilitates informed decision-making, and provides an audit trail of risk management activities.

A. Risk tolerance refers to the level of risk an organization is willing to accept. While important for setting the context for risk management, it isn't a document for recording specific risk details.
B. Risk transfer is a strategy where the risk is shifted to another party, such as through insurance or contracts. While important in risk management, this term refers to a specific response, not a documentation method.
D. Risk analysis is the process of identifying and evaluating risks. The output of the risk analysis (the identified risks and their attributes) is then documented in the risk register.

In essence, the risk register documents the output of risk analysis alongside assigned owners and thresholds.

Authoritative Links:

NIST Risk Management Framework:https://csrc.nist.gov/Projects/risk-management
Project Management Institute (PMI):https://www.pmi.org/ (Search for "Risk Register")

MYEXAM.FR

Question: 30

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

A.Disaster recovery plan

B.Incident response procedure

C.Business continuity plan

D.Change management procedure

Answer: D

Explanation:

Here's a detailed justification for why a change management procedure is the most relevant choice when setting up new firewall rules:

A change management procedure is crucial when implementing new firewall rules because it provides a structured approach to minimize disruptions and potential security risks. Firewalls are critical security components, and any alterations can inadvertently block legitimate traffic or create new vulnerabilities if not properly managed. A change management process includes several essential steps: planning, impact assessment, testing, implementation, documentation, and post-implementation review.

Planning involves defining the purpose of the new rules, identifying the affected systems and services, and outlining the desired outcome. Impact assessment helps determine the potential consequences of the changes, such as service outages or performance degradation. Testing is vital to verify that the new rules function as intended without causing unintended side effects. Implementation involves deploying the changes in a controlled manner, ideally during a maintenance window. Documentation ensures that the changes are recorded for future reference and troubleshooting. Finally, a post-implementation review assesses the success of the changes and identifies any areas for improvement.

Without a change management process, ad-hoc firewall rule modifications can lead to misconfigurations, conflicting rules, and security gaps. These issues can disrupt network operations, expose sensitive data, and violate compliance requirements. Disaster recovery plans, incident response procedures, and business continuity plans are important but address different concerns. While they might be triggered by a firewall-related incident, they are not directly involved in the process of setting up new firewall rules. Therefore, adhering to a change management procedure is the most pertinent action for a security administrator during the implementation of new firewall rules. It ensures that changes are implemented in a controlled, documented, and auditable manner.

Authoritative links:

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems:https://csrc.nist.gov/publications/detail/sp/800-128/final
ITIL 4:https://www.axelos.com/itil (although ITIL is a framework, it provides substantial information on change management).

Question: 31

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A.Open-source intelligence

B.Bug bounty

C.Red team

MYEXAM.FR

D.Penetration testing

Answer: B

Explanation:

The correct answer is B: Bug bounty. Here's why:

A bug bounty program specifically incentivizes external researchers to find and report security vulnerabilities in a company's systems in exchange for compensation. The payout is typically based on the severity and impact of the discovered vulnerability. This aligns perfectly with the scenario described, where individuals are compensated for finding vulnerabilities in the company's internet-facing application.

Open-source intelligence (OSINT), while valuable for threat surface management, is about collecting and analyzing publicly available information. It doesn't directly involve compensating researchers for finding vulnerabilities.

A red team is an internal or contracted team that simulates real-world attacks to test an organization's security defenses. While they do find vulnerabilities, it is not the same as crowdsourcing vulnerability discovery via external researchers with compensation tied to findings.

Penetration testing is a structured and authorized security assessment performed by security professionals to identify vulnerabilities in a specific system or application. While similar to bug bounties in identifying vulnerabilities, penetration testing is typically more formal, targeted, and doesn't rely on open invitations to the broader security research community. The company's decision to allow individuals to test and compensate based on vulnerabilities found distinctly points to a bug bounty program's open and incentivized structure.

Therefore, the best description of the program is a bug bounty. It offers an efficient and cost-effective method for identifying and remediating vulnerabilities.

For further research, consider exploring resources such as:

OWASP (Open Web Application Security Project):https://owasp.org/ Provides information on application security, including bug bounty programs.

Bugcrowd:https://www.bugcrowd.com/ A platform for managing bug bounty programs.

HackerOne:https://www.hackerone.com/ Another platform for bug bounty and vulnerability disclosure programs.

MYEXAM.FR

Question: 32

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A.Insider
B.Unskilled attacker
C.Nation-state
D.Hacktivist

Answer: C

Explanation:

The correct answer is C, Nation-state. Here's why:

Nation-states possess the most significant resources, including financial backing, skilled personnel, and advanced technology, making them capable of launching sophisticated and persistent attacks against critical infrastructure in other countries. These attacks are often driven by geopolitical motives, espionage, or strategic advantage. They might target power grids, communication networks, financial systems, or government agencies.

Insider threats (A) can be dangerous, but their scope and resources are generally limited compared to a nation-state. An unskilled attacker (B) lacks the technical capabilities to mount a complex attack against well-defended critical systems. Hacktivists (D) are motivated by political or social causes, but typically lack the financial and technical resources of a nation-state.

Nation-state actors have the resources for long-term campaigns, extensive reconnaissance, custom malware development, and the ability to circumvent sophisticated security measures. They can afford to purchase zero-day exploits and employ advanced social engineering techniques. The severity of the potential damage resulting from a successful nation-state attack is immense, impacting national security and potentially causing widespread disruption. Their clandestine operations are often difficult to attribute directly, further complicating defense efforts.

For further research, consider exploring resources on nation-state cyberattacks from organizations like:

CISA (Cybersecurity and Infrastructure Security Agency):https://www.cisa.gov/ (Search for reports and analyses on nation-state threats)
ENISA (European Union Agency for Cybersecurity):https://www.enisa.europa.eu/ (Look for threat landscape reports)
MITRE ATT&CK Framework:https://attack.mitre.org/ (Provides a knowledge base of adversary tactics and techniques, many used by nation-states)

Question: 33

Which of the following enables the use of an input field to run commands that can view or manipulate data?

A.Cross-site scripting
B.Side loading
C.Buffer overflow
D.SQL injection

Answer: D

Explanation:

SQL injection (SQLi) is a code injection technique that exploits security vulnerabilities in an application's software. This vulnerability occurs when user-supplied input is improperly incorporated into an SQL query. Attackers can inject malicious SQL code into an input field, causing the application to execute unintended commands.

This injected SQL code can then be used to bypass security measures, such as authentication and authorization, and allows the attacker to access, modify, or delete data stored in the database. For example, an attacker might inject SQL code into a username field to bypass the login process and gain access to an account. They could also modify account balances, steal sensitive information, or even execute arbitrary commands on the database server, depending on the database permissions.

Cross-site scripting (XSS) involves injecting malicious scripts into websites viewed by other users. Side loading refers to installing an application without using an official app store. Buffer overflow exploits occur when a program attempts to write data beyond the allocated buffer, potentially overwriting adjacent memory and disrupting the program's execution or injecting malicious code. While they are security vulnerabilities, they do not directly exploit the use of input fields to run commands that view or manipulate data like SQL

MYEXAM.FR

injection does with databases.

Therefore, SQL injection is the correct answer as it directly allows the attacker to use an input field to run malicious SQL commands that can view, modify, or delete data within a database.

References:

OWASP SQL Injection: https://owasp.org/www-community/attacks/SQL_Injection NIST Definition of SQL Injection: https://csrc.nist.gov/glossary/term/sql-injection

Question: 34

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A.Encrypted

B.Intellectual property

C.Critical

D.Data in transit

Answer: B

Explanation:

The correct answer is B, Intellectual property. Here's why:

Research and development (R&D) units are primarily concerned with creating new knowledge, technologies, and products. The data they work with directly relates to these innovative efforts. This data includes patents, trade secrets, designs, formulas, processes, and other proprietary information, all of which fall under the umbrella of intellectual property (IP). Protecting IP is paramount in R&D to maintain a competitive advantage and prevent unauthorized use or disclosure of the company's innovations.

While other options might be relevant in a broader security context, they are not the most likely type of data used day-to-day in an R&D environment. Encrypted data (A) is a security measure applied to various types of data, but encryption is not inherently the type of data itself. Critical data (C) is a broad term that can encompass many things, but IP is the specific type of critical data central to R&D. Data in transit (D) refers to data being transmitted between locations, which is relevant, but IP constitutes the core content being moved and secured. The training focused on protecting company data in R&D would thus heavily emphasize the handling and security of intellectual property assets. The focus will be how to manage the sensitive information that makes up the company's competitive edge, and therefore must be protected.

Further Reading:

World Intellectual Property Organization (WIPO): https://www.wipo.int/ United States Patent and Trademark Office (USPTO): https://www.uspto.gov/

MYEXAM.FR

Question: 35

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

A.If a security incident occurs on the device, the correct employee can be notified.

B.The security team will be able to send user awareness training to the appropriate device.

C.Users can be mapped to their devices when configuring software MFA tokens.

D.User-based firewall policies can be correctly targeted to the appropriate laptops.

E.When conducting penetration testing, the security team will be able to target the desired laptops.

F.Company data can be accounted for when the employee leaves the organization.

Answer: AF

Explanation:

The correct answer is A and F because labeling laptops with asset inventory stickers and associating them with employee IDs provides several security benefits, primarily improved accountability and incident response.

A. If a security incident occurs on the device, the correct employee can be notified: Linking a device to an employee via inventory and ID allows for quick identification of the user associated with any security incident occurring on that laptop. This is crucial for containing breaches, gathering information, and remediating the issue effectively. Incident responders can directly contact the employee, understand the context surrounding the event, and take appropriate action. This swift identification is essential for minimizing the impact of a security incident.

F. Company data can be accounted for when the employee leaves the organization: When an employee leaves, the asset inventory records linked to their ID provide a clear checklist to ensure all company-issued devices are returned. This prevents potential data leakage or unauthorized access to sensitive information. By knowing which laptop was assigned to which employee, the organization can specifically target data wiping or remote lock procedures if the device is not returned or if there are concerns about data security. This is a critical aspect of offboarding procedures.

Why other options are less suitable:

B.The security team will be able to send user awareness training to the appropriate device: While knowing which employee uses a device could potentially inform targeted training efforts, the device itself is not the primary target for user awareness training; the user is. Employee IDs are more directly linked to user accounts, making those accounts the better choice for targeting training.

C.Users can be mapped to their devices when configuring software MFA tokens: This is a weaker point. While device information might be used for MFA configuration in some very specific and advanced setups, it is not the primary reason for associating assets with employee IDs. MFA is primarily tied to user accounts, not directly to specific devices.

D.User-based firewall policies can be correctly targeted to the appropriate laptops: Similar to B, while potentially helpful, this is not the primary benefit. User-based firewall policies are generally implemented at the network level and associated with user accounts, not directly with device inventory records.

E.When conducting penetration testing, the security team will be able to target the desired laptops: This is relevant only in specific scenarios. The primary goal of asset tracking is not to make penetration testing easier. While knowing which laptop belongs to whom could inform penetration testing scopes, it's a secondary benefit, not a main driver for this practice.

Supporting Resources:

NIST Special Publication 800-53 Revision 5 (Security and Privacy Controls for Information Systems and Organizations): Discusses asset management and control measures. Although not directly about labeling laptops, the concept of comprehensive asset management underpins these practices. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
SANS Institute: Offers various resources on incident response and asset management best practices. Search their website for relevant articles and whitepapers: https://www.sans.org/

In summary, linking laptops to employees via asset inventory and ID stickers mainly improves incident

MYEXAM.FR

response capabilities and facilitates the secure management of company assets during employee offboarding. These are fundamental security practices for any organization.

Question: 36

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

A.Send out periodic security reminders.

B.Update the content of new hire documentation.

C.Modify the content of recurring training.

D.Implement a phishing campaign.

Answer: C

Explanation:

The best option is C, modifying the content of recurring training, because it directly addresses the need to improve situational and environmental awareness as users transition from remote to in-office work. Recurring training provides a consistent and structured platform to reinforce crucial security concepts, adapting existing knowledge to the nuances of the new work environment. Periodic security reminders (A) can be easily overlooked and lack the in-depth instruction necessary to instill behavioral changes. Updating new hire documentation (B) primarily targets new employees, leaving existing employees inadequately informed about relevant security adjustments related to their shift back to the office. While phishing campaigns (D) can test security awareness, they focus more on identifying vulnerabilities than proactively educating users on adapting to a new environment. Recurring training allows for tailored modules focused on physical security, insider threat awareness, social engineering tactics relevant in an office setting, and proper device handling in shared spaces, creating a more effective learning experience and fostering a stronger security culture within the organization during this critical transition. By updating existing training programs, users receive comprehensive instruction that addresses the specific security challenges that arise when moving from remote to in-office work, leading to a more security-conscious workforce and increased environmental awareness.

Further research:

SANS Institute on Security Awareness Training: https://www.sans.org/information-security-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

MYEXAM.FR

Question: 37

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

A.Packet captures

B.Vulnerability scans

C.Metadata

D.Dashboard

Answer: D

Explanation:

The correct answer is **D. Dashboard**. Here's why:

A dashboard is a visual representation of key performance indicators (KPIs) and other relevant metrics. In this scenario, the board member wants a quarterly report on the number of cybersecurity incidents. A dashboard allows the systems administrator to aggregate data from various security tools and systems (SIEM, endpoint protection, firewall logs, etc.) and present it in an easily digestible format for the board. The visual
representation of data through charts, graphs, and tables makes it easier for the board to understand trends, identify risks, and assess the effectiveness of the organization's cybersecurity program at a high level. Packet captures (A) provide detailed network traffic data, which is too granular for the board. Vulnerability scans (B) report potential weaknesses, but don't directly show incident impact. Metadata (C) is data about data and doesn't inherently present the overall incident picture needed for the board. A dashboard specifically helps fulfill the board member's request for a clear and concise overview of incident data.

Authoritative Links for further research:

NIST SP 800-188, Deconstructing the Cybersecurity Supply Chain:
https://csrc.nist.gov/publications/detail/sp/800-188/final (Provides a deep dive into risk frameworks that often lead to developing metrics that can be displayed on a dashboard).

SANS Institute - Security Metrics:https://www.sans.org/information-security/metrics/ (Offers guidance on defining and using security metrics, which are essential components of a cybersecurity dashboard).

MYEXAM.FR

Question: 38

A systems administrator receives the following alert from a file integrity monitoring tool: The
hash of the cmd.exe file has changed.
The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

A.The end user changed the file permissions.

B.A cryptographic collision was detected.

C.A snapshot of the file system was taken.

D.A rootkit was deployed.

Answer: D

Explanation:

The answer is **D. A rootkit was deployed.**

Here's a detailed justification:

The core issue is that the cmd.exe file (the Windows command-line interpreter), a critical system file, has been modified without any legitimate system updates. This indicates malicious tampering.

A rootkit is a type of malware designed to gain privileged access (root or administrator-level control) to a computer system while remaining hidden from detection. One of the primary goals of a rootkit is to maintain persistent and undetectable access. Rootkits often replace or modify essential system utilities like cmd.exe with versions that allow them to execute commands without the user's knowledge or consent, or to hide their presence. This would directly explain a change in the file's hash.

Why the other options are less likely:

A. The end user changed the file permissions: While incorrect file permissions could lead to operational issues, they wouldn't alter the file's hash. The hash is a cryptographic fingerprint of the file's content, not its metadata (like permissions).

B. A cryptographic collision was detected: Cryptographic hash collisions, where two different files produce the same hash value, are exceptionally rare with modern hash algorithms (SHA-256, etc.) used in file integrity monitoring. While theoretically possible, the probability of a collision affecting a system file in this scenario is astronomically low compared to the probability of malware infection. It's not a plausible explanation for a real-world scenario like this.

C. A snapshot of the file system was taken: Taking a snapshot might preserve the state of a compromised file system, but it wouldn't cause the hash of cmd.exe to change. A snapshot simply captures a point-in-time copy.

In summary, the change to cmd.exe without patching strongly points to a malicious intrusion. A rootkit is a common type of malware that specifically targets core system files to maintain persistent access and hide its activities, making it the most likely cause. File integrity monitoring tools are frequently deployed to detect such changes as part of a defense-in-depth security strategy.

Authoritative Links:

Rootkit:https://en.wikipedia.org/wiki/Rootkit
File integrity monitoring:https://www.cisecurity.org/insights/blog/file-integrity-monitoring-fim-explained **Hash collision:**https://owasp.org/www-community/attacks/Collision_attack

Question: 39

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

A.Client
B.Third-party vendor
C.Cloud provider
D.DBA

Answer: A

Explanation:

The correct answer is **A. Client**. In an Infrastructure-as-a-Service (IaaS) model, the shared responsibility model dictates a clear division of security responsibilities. The cloud provider manages the security of the cloud, meaning the underlying infrastructure like physical servers, networking, and storage. However, the client (or customer) is responsible for security in the cloud.

This means the client is responsible for everything they put into the cloud infrastructure. In the case of a database, the client is responsible for hardening the operating system, patching the database software, configuring access controls, encrypting the data, and implementing security measures to prevent vulnerabilities like SQL injection. The cloud provider provides the infrastructure on which the database runs, but the client controls the database's security settings and content.

The DBA, while a crucial role, acts on behalf of the client. They are implementing the client's security policies. The cloud provider isn't generally involved in configuring the client's database security. Third-party vendors might offer security tools, but the ultimate responsibility for the database's security still lies with the client.

IaaS gives the client the most control, which also means the most responsibility. The client has to manage the OS, middleware, runtime, data, and applications. The cloud provider only takes care of virtualization, servers,

MYEXAM.FR

storage, and networking.

For further reading, consult these authoritative resources:

AWS Shared Responsibility Model:https://aws.amazon.com/compliance/shared-responsibility-model/ **Microsoft Azure Shared Responsibility:**https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
Google Cloud Shared Responsibility:https://cloud.google.com/security/compliance/shared-responsibility

Question: 40

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

A.MSA
B.SLA
C.BPA
D.SOW

Answer: D

Explanation:

The correct answer is **D. SOW (Statement of Work)**.

A Statement of Work (SOW) is a document that clearly outlines the scope of work to be performed by a contractor or service provider for a client. It serves as a foundational agreement that details the project's objectives, deliverables, timelines, and costs.

Specifically, a SOW directly addresses the client's request:

Project Outline: The SOW defines the project's purpose, scope, and the tasks involved.
Cost: A detailed breakdown of the project's cost is included in the SOW, often specifying payment terms and milestones.
Completion Time Frame: The SOW sets out the project's timeline, outlining key milestones and the expected completion date.

The other options are incorrect because they do not comprehensively fulfill the client's request:

MSA (Master Service Agreement): An MSA establishes the overall relationship between the client and the service provider but does not contain project-specific details such as cost and timelines. It is more of a framework agreement.
SLA (Service Level Agreement): An SLA defines the level of service expected by the client, typically focusing on metrics like uptime, performance, and response times. It doesn't usually include project scope and costs as comprehensively as an SOW.
BPA (Business Partnership Agreement): A BPA is used to define a partnership between two entities and does not pertain to a client-vendor relationship for project services with defined costs and a timeframe.

In summary, the SOW is the most suitable document because it explicitly outlines the project's scope, cost, and completion time frame, directly addressing the client's requirements.

Here are authoritative links for further research:

Project Management Institute (PMI) - Statement of Work:https://www.pmi.org/ (Search for "Statement of Work" on the PMI website)

MYEXAM.FR

TechTarget - Statement of Work (SOW):
https://www.techtarget.com/searchcompliance/definition/statement-of-work

Question: 41

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A.Secure cookies
B.Version control
C.Input validation
D.Code signing

Answer: C

Explanation:

The correct answer is **C. Input validation**.

Cross-site scripting (XSS) vulnerabilities arise when a web application allows untrusted data (user input) to be injected into the output that it generates. This injected data can then be executed by the victim's browser, potentially allowing an attacker to steal cookies, redirect the user, or deface the website. Input validation is a crucial application security technique that focuses on verifying that the data entered by a user conforms to the expected format, type, length, and allowed characters before it is processed by the application.

By implementing input validation, developers can sanitize user input and prevent malicious code from being injected. This can include techniques like encoding special characters (e.g., converting < to &lt;), blacklisting or whitelisting specific characters or patterns, and ensuring that input adheres to strict data type constraints. Proper input validation at the point of entry (where user input is received) drastically reduces the risk of XSS attacks.

The other options are not direct solutions for XSS:

A. Secure cookies: While secure cookies help protect cookies from being intercepted over non-HTTPS connections, they do not prevent XSS.

B. Version control: Version control is essential for managing code changes but does not directly address application vulnerabilities like XSS.

D. Code signing: Code signing verifies the authenticity and integrity of code, but it primarily protects against tampering with the code itself and doesn't inherently prevent XSS attacks.

Therefore, input validation is the most appropriate application security technique to mitigate XSS vulnerabilities. It's a fundamental practice that should be implemented in any web application to prevent untrusted data from being executed by the browser.

Authoritative Links for Further Research:

OWASP Cross-Site Scripting (XSS):https://owasp.org/www-community/attacks/xss/
OWASP Input Validation Cheat Sheet:https://owasp.org/www-project-cheat-sheets/cheatsheets/Input_Validation_Cheat_Sheet.html

Question: 42

MYEXAM.FR

Which of the following must be considered when designing a high-availability network? (Choose two).

A.Ease of recovery
B.Ability to patch
C.Physical isolation
D.Responsiveness
E.Attack surface
F.Extensible authentication

Answer: AD

Explanation:

The correct answer is A and D: Ease of recovery and Responsiveness. High availability focuses on minimizing downtime and ensuring continuous service operation.

Ease of Recovery: When designing a high-availability network, a robust recovery mechanism is paramount. This includes automated failover systems, comprehensive backup and restoration procedures, and disaster recovery planning. If a component fails, the system should automatically and quickly recover, often switching to a redundant system, to maintain service availability. Without easy recovery, a single point of failure can lead to prolonged downtime, directly contradicting the goals of high availability.

Responsiveness: A highly available system needs to be responsive in multiple aspects. First, the system itself must rapidly respond to requests, even under load or during component failures. Second, the network must respond to changes in demand or failures, rerouting traffic to available resources quickly. Third, the monitoring systems must respond rapidly to anomalies, alerting administrators or triggering automated recovery processes. A slow or unresponsive system defeats the purpose of high availability, as users still experience service disruption.

Options B, C, E, and F, while important for overall security and network design, are not primary considerations for high availability. While patching (B) helps prevent vulnerabilities that could lead to outages, it isn't directly related to uptime. Physical isolation (C) can improve security and reduce the blast radius of an attack but doesn't guarantee continued operation if a component fails. Attack surface reduction (E) is a crucial security principle, but high availability focuses on resilience even if an attack occurs or a component fails. Extensible authentication (F) enhances security but doesn't inherently contribute to minimizing downtime.

In essence, options A and D ensure the system can withstand failures and maintain functionality with minimal disruption, which aligns directly with the core principles of high availability.

Authoritative links:

Microsoft Azure High Availability:https://learn.microsoft.com/en-us/azure/architecture/framework/resiliency/design
AWS High Availability:https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/pillar/reliability.en.html
Google Cloud High Availability:https://cloud.google.com/architecture/high-availability-systems-google-cloud

Question: 43

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

A.Air gap the system.
B.Move the system to a different network segment.

MYEXAM.FR

C.Create a change control request.

D.Apply the patch to the system.

Answer: C

Explanation:

The correct first step when applying a high-priority patch to a production system is to **C. Create a change control request.**

Change control is a crucial IT service management (ITSM) process, especially within cloud and on-premises environments, ensuring changes are implemented methodically and with minimal disruption. Before any modification to a production system, especially a critical one like patching, a formal change request should be submitted.

This request details the proposed change (patch application), the justification for the change (high priority security vulnerability), the potential impact on the system and related services, a rollback plan in case of failure, and a communication plan to notify stakeholders. This structured approach allows for proper evaluation and risk assessment before making live system alterations. Skipping change control could lead to unintended consequences such as system instability, service outages, or compatibility issues.

While air-gapping or segmenting might seem like good security measures, they don't precede the change management process itself. Air gapping the system(option A) immediately cuts off all network connectivity to the system and therefore, is too drastic a first step without proper approval. Moving the system to a separate network segment (option B) is a good practice in some situations but is also not the first priority. Directly applying the patch (option D) without proper planning is reckless and introduces unnecessary risk. Change control facilitates collaboration and ensures that all stakeholders are aware and prepared for the patch deployment.Therefore, initiating a formal change control request is paramount to mitigating risks and preserving system integrity.https://www.atlassian.com/itsm/change-managementhttps://www.bmc.com/blogs/change-management-process/

Question: 44

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

A.To gather IoCs for the investigation

B.To discover which systems have been affected

C.To eradicate any trace of malware on the network

D.To prevent future incidents of the same nature

Answer: D

Explanation:

Root cause analysis (RCA) is crucial in incident response because it goes beyond simply addressing the immediate symptoms of a security breach. It aims to uncover the underlying reasons why an incident occurred in the first place. By identifying these root causes, organizations can implement preventative measures to minimize the likelihood of similar incidents happening again. This proactive approach improves the overall security posture, saving resources and reducing potential damage in the long run.

Gathering Indicators of Compromise (IoCs) is essential for threat hunting and future incident detection, but it doesn't prevent recurrence. Discovering affected systems helps contain the incident, but doesn't address the reason for the breach. Eradicating malware eliminates the immediate threat, but without addressing

MYEXAM.FR

vulnerabilities or security gaps, the system remains vulnerable.

RCA helps determine weaknesses in security controls, configuration errors, inadequate patching, or insufficient security awareness training. Correcting these underlying issues provides a lasting improvement in the security posture. RCA benefits cloud environments as it allows organizations to identify
misconfigurations, IAM permission issues, and other cloud-specific vulnerabilities that could lead to future incidents. RCA findings may also inform security policies and procedures, automation scripts, and cloud infrastructure design.

For further research, consult resources like the SANS Institute's Incident Handler's Handbook and NIST's Computer Security Incident Handling Guide.

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

M/EXAM.FR

Question: 45

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

A.Fines
B.Audit findings
C.Sanctions
D.Reputation damage

Answer: B

Explanation:

The most likely immediate outcome of a large bank failing an internal PCI DSS compliance assessment is **Audit findings**. Here's why:

Internal PCI DSS assessments are designed to identify gaps and weaknesses in a bank's security posture concerning cardholder data. If the bank fails, the immediate result will be a detailed report outlining the areas where the bank is non-compliant. This report constitutes the "audit findings." These findings then trigger a remediation process.

While other options are potential consequences, they are not the immediate outcome.

A. Fines: Fines are generally levied by the payment card brands (Visa, Mastercard, etc.) or acquiring banks after a more formal external audit reveals non-compliance, especially after repeated failures or breaches resulting from non-compliance. An internal audit failing does not directly trigger fines, but exposes the bank to the risk of future fines if not addressed.

C. Sanctions: Similar to fines, sanctions (e.g., losing the ability to process certain card types) are imposed by payment card brands or regulators and are not the direct result of an internal assessment. The bank's acquirer bank might impose sanctions if non-compliance persists and poses an unacceptable risk.

D. Reputation damage: Reputation damage is a potential consequence of a data breach or public disclosure of non-compliance. An internal failure is, initially, a private matter. However, if the bank does not rectify the issues identified, and a breach occurs as a result, then reputation damage will likely ensue.

Therefore, an internal PCI DSS assessment failure directly results in the generation of **Audit findings**, which is the most immediate and likely outcome. These findings serve as the basis for corrective actions to ensure compliance and avoid future penalties. The bank must address those findings in order to not be exposed to fines, sanctions, or reputation damage down the line.

Relevant links:

PCI Security Standards Council: https://www.pcisecuritystandards.org/
Understanding PCI DSS Requirements: https://www.pcicomplianceguide.org/pci-faqs-2/

Question: 46

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

A.Capacity planning
B.Redundancy
C.Geographic dispersion
D.Tabletop exercise

Answer: A

Explanation:

The best answer is A, Capacity Planning. Let's break down why:

Capacity planning is the process of determining the production capacity needed by an organization to meet changing demands for its products or services. In a business continuity context, capacity planning involves understanding the minimum resources, including personnel, infrastructure, and services, required to maintain essential business functions during and after a disruption. This directly relates to the question's focus on determining the required staff to "sustain the business." The organization must plan for the minimal acceptable level of capacity after a disruption.

Redundancy (Option B) focuses on having duplicate systems or components to ensure availability, but doesn't specifically address the number of staff required for business continuity. Geographic dispersion (Option C) involves distributing resources across different locations to mitigate the impact of a localized event, but doesn't quantify staffing needs. A tabletop exercise (Option D) is a simulation to test a business continuity plan, but it's not the step that determines the minimum required staffing level.

Capacity planning directly helps to answer questions such as: What is the minimum number of employees to keep the business functional? What is the minimum IT infrastructure to maintain critical applications? The results of capacity planning will then inform the redundancy, geographic dispersion, and tabletop exercises performed by the organization.

Therefore, determining the number of staff members required to sustain the business is a core component of capacity planning within a business continuity strategy.

For further reading on capacity planning in the context of disaster recovery and business continuity, consider these resources:

TechTarget's definition of Capacity Planning:
https://www.techtarget.com/searchdatacenter/definition/capacity-planning
IBM's resources on Capacity Planning:https://www.ibm.com/topics/capacity-planning (Although focusing on IT infrastructure, it illustrates core principles)

Question: 47

A company’s legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective

MYEXAM.FR

way to limit this access?

A.Data masking
B.Encryption
C.Geolocation policy
D.Data sovereignty regulation

Answer: C

Explanation:

The most effective solution for restricting access to sensitive documents in a SaaS application based on the user's geographic location is implementing a geolocation policy. Here's why:

Geolocation policies directly control access based on geographic location. These policies are configured to allow or deny access to resources based on the originating IP address or other geolocation data of the user. This aligns directly with the requirement to block users from high-risk countries.

Data masking hides sensitive data within documents, but it doesn't prevent users from high-risk countries from accessing the document in the first place. Masking is primarily for compliance and security within authorized access scenarios, not for initial access control based on location.

Encryption protects data confidentiality while in transit or at rest but doesn't inherently prevent unauthorized access based on location. While encryption is crucial for data security, it doesn't address the specific access control requirement outlined in the scenario. Once a user has the decryption key and authorization to access the encrypted data, encryption won't prevent their use based on geographic origin.

Data sovereignty regulation refers to laws governing where data must reside. While important for compliance, it doesn't directly enforce access controls based on the user's location. It focuses on the physical location of the data storage, not the user's point of access.

Therefore, a geolocation policy provides the most direct and effective means of controlling access to the documents based on the user's geographic location, fulfilling the legal department's requirement.

Authoritative Links:

Cloudflare Geolocation:https://www.cloudflare.com/learning/cdn/glossary/geolocation/
Microsoft Azure Conditional Access (Geolocation):https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question: 48

Which of the following is a hardware-specific vulnerability?

A.Firmware version
B.Buffer overflow
C.SQL injection
D.Cross-site scripting

Answer: A

Explanation:

The correct answer is A. Firmware version. Here's why:

MYEXAM.FR

Firmware resides directly on hardware devices, providing low-level control and instructions for the hardware's operation. Vulnerabilities in firmware are tied to the specific hardware on which it runs. An outdated or improperly configured firmware version can expose a device to known exploits.

A buffer overflow (B) is a software vulnerability where data exceeds the allocated buffer size, potentially leading to code execution. SQL injection (C) is a web application vulnerability that allows attackers to inject malicious SQL code into database queries. Cross-site scripting (D) is another web application vulnerability where attackers inject malicious scripts into websites viewed by other users.

While buffer overflows, SQL injection, and cross-site scripting can affect systems that rely on specific hardware, they are not inherently hardware-specific. They are software-level flaws. Firmware vulnerabilities, however, are inherently linked to the particular hardware's BIOS or embedded system instructions. If a specific hardware component has a faulty firmware version, all systems using that component could be vulnerable until the firmware is updated. This makes the vulnerability hardware-dependent. For example, vulnerabilities in Intel Management Engine (IME) firmware directly impact Intel processors.

Therefore, the only option that is a hardware-specific vulnerability is A.

Reference Links:

NIST definition of Firmware: https://csrc.nist.gov/glossary/term/firmware
OWASP Buffer Overflow: https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
OWASP SQL Injection: https://owasp.org/www-community/attacks/SQL_Injection
OWASP Cross-site Scripting (XSS): https://owasp.org/www-community/attacks/xss/

Question: 49

While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.
Which of the following actions would prevent this issue?

A.Documenting the new policy in a change request and submitting the request to change management
B.Testing the policy in a non-production environment before enabling the policy in the production network
C.Disabling any intrusion prevention signatures on the “deny any” policy prior to enabling the new policy
D.Including an “allow any” policy above the “deny any” policy

Answer: B

Explanation:

The correct answer is **B. Testing the policy in a non-production environment before enabling the policy in the production network.**

Here's why:

The core issue is introducing a "deny any" rule without understanding its full impact. Firewalls process rules in order, so a "deny any" rule at the bottom effectively blocks all traffic that hasn't already been explicitly allowed. This can unintentionally block legitimate and necessary traffic, as seen with the unreachable servers.

Testing in a non-production environment (a test lab or staging environment) is crucial for several reasons:

Risk Mitigation: It allows you to identify unintended consequences before they affect live systems and users. By simulating production traffic, you can observe the effects of the new policy.

Validation: It confirms that the policy functions as intended. You can verify that the allowed traffic is indeed permitted and that the denied traffic is blocked.

MYEXAM.FR

Refinement: It provides an opportunity to fine-tune the policy. If the initial tests reveal problems, you can adjust the rules to achieve the desired security posture without disrupting operations.

Reduced Downtime: Production downtime caused by misconfigured rules can be costly. Testing minimizes the likelihood of such incidents.

Option A is important for change management, but it doesn't prevent the issue; it merely documents it. Option C relates to intrusion prevention, which is a different aspect of security. Option D essentially negates the "deny any" policy's purpose, rendering it ineffective.

By testing the firewall policy in a controlled, non-production environment, the technician can identify and rectify the problem before it disrupts the company's servers, preventing the outage.

Authoritative Links:

NIST Guide to Firewall Technologies: (Although somewhat dated, the concepts are still relevant) - https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/archive (Search for firewall testing best practices.) **SANS Institute Reading Room: Firewall Management: -** https://www.sans.org/reading-room/whitepapers/firewalls/firewall-management-36424 (Look for sections discussing testing and change control.)

Question: 50

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

A.Real-time recovery

B.Hot

C.Cold

D.Warm

Answer: D

Explanation:

The correct answer is **D. Warm**. Here's why:

A "warm" site provides a balance between cost and recovery time objectives (RTO) and recovery point objectives (RPO). It's a partially operational backup facility containing hardware and software but might lack up-to-date data. This aligns perfectly with the organization's requirement for cost-benefit as the primary driver and a two-day RTO/RPO. Setting up and maintaining a warm site is less expensive than a hot site because it doesn't require real-time data replication or constant synchronization.

Cold Site: This is the least expensive option, essentially just a shell of a facility with basic infrastructure like power and cooling. Populating it with hardware, software, and data takes considerable time, far exceeding the two-day RTO/RPO.

Hot Site: This is the most expensive option. It's a fully operational, mirrored environment with near real-time data replication. While it offers minimal RTO/RPO, it's not cost-effective given the organization's requirements.

Real-time Recovery: This isn't a type of site but a recovery strategy typically associated with hot sites where failover happens almost instantaneously.

A warm site offers a middle ground. The organization would pre-install essential hardware and software but likely perform periodic data replication rather than continuous replication, saving costs. When a disaster occurs, the warm site can be brought online within the two-day window by restoring the latest data backups. This approach balances cost-effectiveness with acceptable recovery times.

MYEXAM.FR

Essentially, it's about cost versus recovery speed. Since cost is the primary concern and a two-day RTO/RPO is acceptable, a warm site is the most sensible choice, offering a compromise between minimal cost and acceptable downtime.

Authoritative Links for Further Research:

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final (While slightly dated, this provides fundamental concepts on business continuity and disaster recovery planning, including different site types.)
TechTarget Definition - Warm Site:https://www.techtarget.com/searchdisasterrecovery/definition/warm-site (Provides a clear and concise definition of a warm site and its characteristics.)

MYEXAM.FR

Question: 51

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

A.Enumeration
B.Sanitization
C.Destruction
D.Inventory

Answer: B

Explanation:

The correct answer is **B. Sanitization**.

Sanitization, in the context of data security, refers to the process of permanently removing or destroying data stored on a storage device, such as a hard drive, in a way that renders the data unrecoverable. The policy described directly aligns with this definition, as it necessitates the secure wiping of hard drives prior to disposal. This ensures confidential information is not exposed during the recycling process.

Enumeration (A) is the process of discovering usernames, network resources and services on a system. This is a reconnaissance step used by attackers. Destruction (C) involves physically destroying the storage media, such as shredding or pulverizing the hard drive. While effective, it's more drastic than simply wiping the drives and might be unnecessary if the goal is to comply with recycling policies after secure data removal. Inventory (D) is simply tracking assets, like computers or hard drives.

Secure wiping using software-based methods overwrites the existing data with random patterns multiple times, making it exceedingly difficult, if not impossible, to retrieve the original data. Sanitization goes beyond simple deletion; it actively removes data remnants. This is critical for compliance with data privacy regulations (like GDPR, CCPA, HIPAA) and protecting sensitive information. The company's requirement demonstrates a proactive approach to data security and adherence to responsible data disposal practices. The goal is to securely remove data and comply with recycling processes.

Reference Links:

NIST Guidelines for Media Sanitization:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
Data Sanitization Methods:https://searchdatabackup.techtarget.com/definition/data-sanitization

Question: 52

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A.Private
B.Critical
C.Sensitive
D.Public

Answer: C

Explanation:

The correct answer is **C. Sensitive**. Here's a detailed justification:

Patient data, often referred to as Protected Health Information (PHI), requires a high level of protection due to its potential for causing significant harm if disclosed or compromised. Data classification schemes are used to categorize data based on its sensitivity and impact, determining the appropriate security controls. In this context, "Sensitive" is the most fitting classification.

Sensitive data typically includes information that, if disclosed without authorization, could cause significant damage or harm to individuals or the organization. Medical records, treatment information, social security numbers, and other patient identifiers fall squarely into this category. Unauthorized disclosure could lead to identity theft, reputational damage, legal ramifications (such as HIPAA violations in the US), and
discrimination.

Private data is generally personal information that individuals expect to be kept confidential, but the consequences of its disclosure may be less severe than those for sensitive data. While some patient data could be considered private, the healthcare context necessitates a higher level of protection.

Critical data is essential for the organization's survival and operations. While patient data is certainly crucial for healthcare delivery, it's the sensitivity aspect that primarily drives the security requirements. Data related to financial viability or key operational processes would be more likely classified as critical.

Public data is information freely available to anyone and requires minimal protection. Patient data is explicitly not public.

Therefore, the "Sensitive" classification accurately reflects the need to implement stringent security measures, such as encryption, access controls, audit logging, and data loss prevention (DLP) mechanisms, to protect patient information from unauthorized access, use, or disclosure. This classification triggers policies and procedures that ensure compliance with healthcare regulations like HIPAA, GDPR (if applicable to the hospital's operations), and other relevant data protection laws. The use of robust security measures directly aligns with the requirements for handling sensitive data within a healthcare environment.

For further research, refer to:

1. **NIST Special Publication 800-171**: Provides guidance on protecting controlled unclassified information (CUI) in nonfederal systems and organizations, which often includes sensitive data. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
2. **HIPAA Security Rule**: Outlines the administrative, physical, and technical safeguards required to protect electronic protected health information (ePHI). https://www.hhs.gov/hipaa/for-professionals/security/index.html

Question: 53

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the

MYEXAM.FR

following should the hosting provider consider first?

A.Local data protection regulations
B.Risks from hackers residing in other countries
C.Impacts to existing contractual obligations
D.Time zone differences in log correlation

Answer: A

Explanation:

The correct answer is **A. Local data protection regulations.**

When a U.S.-based cloud hosting provider expands its data centers internationally, the paramount concern should be adhering to the data protection regulations of each new location. This is because data protection laws vary significantly across countries and regions. Failing to comply with these regulations can result in hefty fines, legal repercussions, and reputational damage.

Examples include GDPR in Europe, CCPA in California, and various national laws globally. These regulations dictate how personal data can be collected, processed, stored, and transferred. They also address data subject rights, such as the right to access, rectification, and erasure of data.

Before establishing a data center in a new country, the provider must conduct thorough legal research to understand the local data protection landscape. This includes identifying the relevant laws and regulations, understanding the requirements for data localization (where data must be stored within the country), and implementing appropriate security measures to protect data.

While other factors like risks from hackers in other countries (B), impacts on existing contractual obligations (C), and time zone differences in log correlation (D) are important, they are secondary to legal compliance. Security risks can be addressed with appropriate security controls, contract modifications can be negotiated, and log correlation issues can be mitigated with appropriate tools and processes. However, violating local data protection regulations presents an immediate and significant legal risk.

Therefore, understanding and complying with local data protection regulations is the most critical initial consideration for a cloud hosting provider expanding internationally. Ignoring these regulations could lead to severe penalties and business disruptions.

Supporting Links:

General Data Protection Regulation (GDPR):https://gdpr-info.eu/
California Consumer Privacy Act (CCPA):https://oag.ca.gov/privacy/ccpa
Cloud Security Alliance (CSA):https://cloudsecurityalliance.org/ - Offers resources on data privacy and compliance in the cloud.

MYEXAM.FR

Question: 54

Which of the following would be the best way to block unknown programs from executing?

A.Access control list
B.Application allow list
C.Host-based firewall
D.DLP solution

Answer: B

Explanation:

The best method to prevent execution of unknown programs is an application allow list. An application allow list, sometimes referred to as application whitelisting, is a security approach that explicitly defines which applications are permitted to run on a system. This implies that only applications on the approved list can execute, blocking all others, including unknown or potentially malicious programs.

Access control lists (ACLs) primarily regulate network traffic based on source and destination IP addresses, ports, and protocols, not the applications themselves. Host-based firewalls offer broader protection by monitoring network traffic entering and leaving a specific host, but typically rely on rules based on ports and protocols and do not inherently prevent the execution of unknown applications. Data Loss Prevention (DLP) solutions focus on preventing sensitive data from leaving an organization's control, rather than controlling application execution.

By contrast, application allow listing ensures a highly restrictive environment, ideal for scenarios requiring maximum security. Its effectiveness stems from its "default deny" approach, where everything is blocked unless explicitly allowed. Although initial setup and maintenance of an application allow list can be demanding, requiring thorough application inventory and ongoing updates, it significantly reduces the attack surface by preventing unknown and potentially malicious software from running. Implementing an application allow list ensures a proactive security posture by preventing threats before they can execute, aligning with the principle of least privilege.

Further resources:

NIST Guide to Application Whitelisting:https://csrc.nist.gov/Projects/application-whitelisting **SANS Institute on Application Whitelisting:**https://www.sans.org/white-papers/33527/

Question: 55

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?

A.White
B.Purple
C.Blue
D.Red

Answer: D

Explanation:

The correct answer is **D. Red**.

Here's a detailed justification:

A red team is a group of security professionals who play the role of attackers to test an organization's security posture. Their primary objective is to identify vulnerabilities and weaknesses in systems, networks, applications, and even human behavior through simulated attacks. Penetration testing and social engineering are core activities of a red team engagement. Penetration testing involves actively attempting to exploit vulnerabilities in systems and networks to gain unauthorized access. Social engineering focuses on manipulating individuals into divulging sensitive information or performing actions that compromise security.

White teams are often involved in overseeing red and blue team exercises and defining the rules of engagement. Purple teams seek to blend red and blue team functions, facilitating knowledge sharing and

MYEXAM.FR

improving both defensive and offensive capabilities. Blue teams are the internal security teams responsible for defending against attacks.

Given that the scenario involves penetration testing and social engineering as offensive security assessment activities, the red team is the most appropriate choice. They are specifically trained and equipped to simulate real-world attacks and identify security gaps. The consultant's actions directly align with a red team's function.

Authoritative Links:

NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
SANS Institute - Red Team vs. Blue Team:https://www.sans.org/blog/red-team-vs-blue-team/

MYEXAM.FR

Question: 56

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A.Testing input validation on the user input fields
B.Performing code signing on company-developed software
C.Performing static code analysis on the software
D.Ensuring secure cookies are use

Answer: B

Explanation:

The most appropriate solution for ensuring the authenticity of code created by a company is performing code signing. Code signing involves digitally signing the software with a certificate that verifies the software's origin and integrity. This process assures users that the code hasn't been tampered with since it was signed by the identified developer. When a user downloads and attempts to run signed code, the operating system can verify the digital signature against a trusted certificate authority. If the signature is valid, the user can be confident that the code is genuine. This helps prevent the execution of malicious or altered software, fostering trust and enhancing security.

Option A (Testing input validation) focuses on preventing vulnerabilities arising from user input and is not directly related to code authenticity. Option C (Static code analysis) can identify potential security flaws and coding errors, but doesn't authenticate the code's source. Option D (Ensuring secure cookies) addresses web application security by protecting session data but doesn't verify code authenticity. Only code signing offers a mechanism to establish and verify the code's origin and integrity.

For further research, consider reviewing the following resources:

Microsoft's Code Signing:https://learn.microsoft.com/en-us/windows-hardware/drivers/install/digital-signatures
OWASP on Code Signing:https://owasp.org/www-project-code-signing/

Question: 57

Which of the following can be used to identify potential attacker activities without affecting production servers?

A.Honeypot

B.Video surveillance

C.Zero Trust

D.Geofencing

Answer: A

Explanation:

The correct answer is A. Honeypots are designed to mimic real systems but are intentionally vulnerable. Their primary purpose is to attract attackers, allowing security teams to observe and analyze malicious activity in a controlled environment without putting production assets at risk. Any interaction with a honeypot indicates unauthorized activity since legitimate users should never interact with it. This early detection helps in understanding attacker tactics, techniques, and procedures (TTPs).

Video surveillance (B) is focused on physical security and does not directly identify attacker activities in the digital realm. Zero Trust (C) is a security framework based on the principle of "never trust, always verify," which aims to secure all resources regardless of location but does not inherently identify specific attacker behaviors. Geofencing (D) creates virtual boundaries and can trigger alerts when devices enter or exit defined areas, primarily useful for location-based security but not directly suited for identifying network-based attacker activities. Therefore, a honeypot effectively fulfills the purpose of identifying potential malicious activities without impacting real production servers because its sole purpose is to be a decoy, attracting and trapping attackers. The other options are simply not designed for this purpose.

Further reading:

SANS Institute on Honeypots: https://www.sans.org/information-security/glossary/honeypot NIST definition of Honeypots: https://csrc.nist.gov/glossary/term/honeypot

MYEXAM.FR

Question: 58

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

A.Analysis

B.Lessons learned

C.Detection

D.Containment

Answer: A

Explanation:

The correct answer is **A. Analysis**. Here's why:

Analysis, in the context of incident response, involves a deep dive into the incident to understand its nature, scope, cause, and impact. This phase aims to determine what happened, how it happened, and who or what was responsible. Specifically, identifying the source of the incident falls directly within the analysis activity.

The incident response team meticulously examines logs, network traffic, system configurations, and other relevant data to trace the incident back to its origin. This can involve identifying a compromised user account, a vulnerable application, a malicious file, or a network misconfiguration.

Option B, Lessons learned, is a post-incident activity focused on documenting what worked well, what didn't, and how to improve future incident response efforts. It comes after the immediate incident has been handled.

Option C, Detection, refers to the process of recognizing that an incident has occurred. While related, it precedes analysis. Detection triggers the incident response process, while analysis investigates the details after an incident has been detected.

Option D, Containment, focuses on limiting the damage caused by the incident and preventing it from spreading further. While important, it's a different activity than determining the source.

In summary, the analysis phase is the specific activity that focuses on determining the root cause and source of an incident. Identifying the source is a fundamental objective during analysis to better understand the incident's overall impact.For further research, consider these resources:

NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Provides a comprehensive overview of incident handling and analysis)
SANS Institute:https://www.sans.org/ (Offers various courses and resources on incident response and security analysis)

MYEXAM.FR

Question: 59

A security practitioner completes a vulnerability assessment on a company’s network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

A.Conduct an audit.
B.Initiate a penetration test.
C.Rescan the network.
D.Submit a report.

Answer: C

Explanation:

The most logical next step after remediating vulnerabilities found in a vulnerability assessment is to rescan the network (C). This verifies that the remediation efforts were successful and that the identified vulnerabilities have indeed been addressed. Simply submitting a report (D) without verification wouldn't confirm the effectiveness of the fixes. While an audit (A) is valuable, it usually encompasses a broader scope than just the specific vulnerabilities addressed in the remediation. A penetration test (B) is also beneficial, but it's more effective after verifying the basic fixes with a rescan. Rescanning provides immediate feedback on the remediation's success. It identifies if any fixes were incomplete or caused new vulnerabilities. This iterative process of assessment, remediation, and rescanning is crucial for continuous security improvement. It ensures that the security posture is actively maintained, leading to a reduced attack surface. This process aligns with the principle of continuous monitoring and improvement, essential for modern security practices.

Delaying verification can leave systems vulnerable even after remediation efforts, negating the purpose of the initial assessment. Rescanning helps build confidence in the security controls and allows for quick follow-up actions if necessary. This also helps to prioritize further security activities, such as penetration testing, by focusing on areas where remediation may have been less effective. In short, rescanning confirms the effectiveness of the remediation efforts and helps prevent the re-emergence of the same vulnerabilities.

Relevant links for more information on vulnerability management and security best practices:

NIST Vulnerability Management:https://csrc.nist.gov/Projects/vulnerability-management **SANS Institute on Vulnerability Scanning:**https://www.sans.org/white-papers/36341/

Question: 60

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.
Which of the following best describes the user's activity?

A.Penetration testing

B.Phishing campaign

C.External audit

D.Insider threat

Answer: D

Explanation:

The user's activity is best described as an insider threat. An insider threat refers to a security risk originating from within the organization, often involving employees, former employees, contractors, or business associates who have access to internal systems and data.

In this scenario, the user leveraged legitimate access (remote login) to perform unauthorized activities (copying large amounts of data to a personal device after hours). This clearly indicates a potential violation of data security policies and a possible intention to misuse or exfiltrate sensitive information.

Penetration testing is a planned, authorized assessment of security vulnerabilities, which does not align with the surreptitious nature of the described activity. A phishing campaign involves deceiving individuals to gain access, which is not the case here as the user already had authorized access. An external audit is a review conducted by an independent entity, not an activity performed by a user with pre-existing access.

Insider threats pose a significant risk because insiders often have privileged access and knowledge of organizational systems, making it easier for them to bypass security controls and cause damage. This scenario demonstrates a classic example of such a threat.

Further research on insider threats can be found at:

Carnegie Mellon University, Software Engineering Institute:https://www.sei.cmu.edu/our-work/insider-threat/
CISA (Cybersecurity & Infrastructure Security Agency):https://www.cisa.gov/insider-threats

MYEXAM.FR

Question: 61

Which of the following allows for the attribution of messages to individuals?

A.Adaptive identity

B.Non-repudiation

C.Authentication

D.Access logs

Answer: B

Explanation:

The correct answer is B, Non-repudiation. Non-repudiation ensures that the sender of a message or performer of an action cannot deny having sent the message or performed the action. This relies on cryptographic methods, often involving digital signatures, to create undeniable proof of origin. Therefore, non-repudiation directly addresses the requirement of attributing messages to specific individuals.

Adaptive identity, while valuable for security, dynamically adjusts access based on context, but does not provide definitive proof of origin. Authentication verifies a user's identity but doesn't guarantee they can't deny sending a message after being authenticated. Access logs record events, but without cryptographic proof, they might be tampered with or disputed. Non-repudiation establishes trust in the integrity and origin of the message, crucial for accountability and legal admissibility. This mechanism ensures the sender is undeniably linked to the sent message or performed action. Digital signatures, often used to implement non-repudiation, provide verifiable proof that a message has not been altered and was sent by the claimed sender.

Without non-repudiation, it becomes challenging to establish accountability, particularly in sensitive transactions or communications.

For further reading, see:

NIST definition: https://csrc.nist.gov/glossary/term/nonrepudiation
TechTarget definition: https://www.techtarget.com/searchsecurity/definition/nonrepudiation

MYEXAM.FR

Question: 62

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

A.Automation
B.Compliance checklist
C.Attestation
D.Manual audit

Answer: A

Explanation:

The best method for daily monitoring of server security setting modifications is automation (A). Here's why:

Scale and Frequency: Manually auditing servers daily is resource-intensive, time-consuming, and impractical, especially with numerous servers. Automation allows for consistent, scalable, and frequent checks.

Real-time Detection: Automated tools can continuously monitor configurations and detect deviations from baseline settings in near real-time. This rapid detection allows for quick remediation.

Accuracy and Consistency: Human error is inherent in manual processes. Automated systems, when properly configured, offer a higher degree of accuracy and consistency in detecting changes.

Reduced Operational Overhead: Automation minimizes the need for manual intervention, freeing up security personnel to focus on more strategic tasks like threat analysis and incident response.

Configuration Management: Automation leverages configuration management tools that can define and enforce desired states for server security settings. Any drift from this desired state triggers an alert.

Auditing and Reporting: Automated systems generate detailed logs and reports on configuration changes, providing an audit trail for compliance and security investigations.

Compliance Integration: Many automation tools integrate with compliance frameworks, ensuring that security settings align with industry standards and regulatory requirements.

DevSecOps: Automation is a cornerstone of DevSecOps, enabling security to be integrated into the software development lifecycle, including infrastructure configuration management.

Infrastructure as Code (IaC): IaC principles involve defining infrastructure configurations as code. Automation uses these code definitions to provision and manage server settings, ensuring consistency.

Compliance checklists (B) are useful for periodic assessments but are not suitable for daily, real-time monitoring. Attestation (C) is more about verifying claims of compliance, not continuous monitoring. Manual audits (D), as explained earlier, are impractical for daily checks across multiple servers. Automation is a more practical, scalable, and efficient approach.

Authoritative Links:

NIST Guidelines on Configuration Management: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf **SANS Institute on Automation:**https://www.sans.org/white-papers/4134/

Question: 63

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A.SCAP

B.NetFlow

C.Antivirus

D.DLP

Answer: D

Explanation:

The correct answer is **D. DLP (Data Loss Prevention)**.

DLP tools are specifically designed to detect and prevent sensitive data, such as Personally Identifiable Information (PII), from leaving an organization's control. These tools work by inspecting data in transit (e.g., emails, file transfers), data at rest (e.g., files stored on servers or endpoints), and data in use (e.g., data being accessed or processed by applications). In the context of the question, a DLP system would scan outgoing emails for patterns or keywords that indicate the presence of PII, such as social security numbers, credit card numbers, or medical records. If a match is found, the DLP system can take various actions, such as blocking the email, quarantining the file, or alerting security personnel.

SCAP (Security Content Automation Protocol) is a framework for automating security vulnerability management and policy compliance assessment. While useful for overall security posture, it doesn't directly monitor data exfiltration. (NIST: https://csrc.nist.gov/projects/security-content-automation-protocol)

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network flow data. It provides insights into network traffic patterns but doesn't analyze the content of data being transmitted, making it unsuitable for detecting PII.

Antivirus software is designed to detect and remove malicious software, such as viruses, worms, and Trojans. While it can protect against data breaches caused by malware, it's not designed to specifically detect and prevent the accidental leakage of PII via email. (e.g., Emsisoft: https://www.emsisoft.com/en/antivirus/)

DLP solutions often employ techniques like keyword analysis, regular expression matching, data fingerprinting, and machine learning to accurately identify sensitive data. Many DLP tools can be integrated with email gateways, cloud storage services, and endpoint devices to provide comprehensive data protection.

By implementing DLP, organizations can significantly reduce the risk of accidental data breaches and maintain compliance with regulations like GDPR, HIPAA, and CCPA.

Question: 64

An organization recently updated its security policy to include the following statement:
Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.

MYEXAM.FR

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

A.Identify embedded keys
B.Code debugging
C.Input validation
D.Static code analysis

Answer: C

Explanation:

The correct answer is **C. Input validation**.

The organization is using regular expressions to sanitize user inputs received from web forms. This process specifically targets potentially malicious special characters often used in injection attacks. This aligns directly with the concept of input validation, which is a critical security practice aimed at preventing attackers from injecting malicious code or commands into an application. By removing these characters, the organization is actively mitigating the risk of vulnerabilities like SQL injection, command injection, or cross-site scripting (XSS).

The other options are less directly related. Identifying embedded keys (A) is about secrets management, not sanitizing input data. Code debugging (B) is a broader process of finding and fixing errors, not a specific security technique. Static code analysis (D) involves examining source code for potential vulnerabilities without executing the code, which is a preventative measure, but the provided statement specifically targets runtime input handling. Regular expressions focus on inspecting user-supplied data as it enters the system, making input validation the most relevant technique described. Input validation is essential to ensure that only legitimate data reaches the application's backend, preventing potential compromise.

For further research, refer to the following resources:

OWASP Input Validation Cheat Sheet: https://owasp.org/www-project-cheat-sheets/cheatsheets/Input_Validation_Cheat_Sheet.html
SANS Institute on Input Validation: https://www.sans.org/blog/input-validation-techniques-vulnerabilities/

MYEXAM.FR

Question: 65

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

A.Place posters around the office to raise awareness of common phishing activities.
B.Implement email security filters to prevent phishing emails from being delivered.
C.Update the EDR policies to block automatic execution of downloaded programs.
D.Create additional training for users to recognize the signs of phishing attempts.

Answer: C

Explanation:

The correct answer is C: Update the EDR policies to block automatic execution of downloaded programs. Here's why:

The primary goal is to reduce the impact after a user clicks a phishing link. While training and awareness (A and D) are crucial for prevention, they don't address the damage caused by a successful click. Email filters (B) aim to prevent the phishing email from reaching the user in the first place, but aren't foolproof.

Updating the EDR (Endpoint Detection and Response) policies directly tackles the consequences of a user clicking a malicious link. Phishing emails often trick users into downloading malware or executing malicious scripts. EDR systems are designed to monitor endpoints (computers, servers) for suspicious activity and block threats. By updating the policies to prevent automatic execution of downloaded programs, the analyst can significantly limit the impact of a successful phishing attack. Even if a user clicks the link and downloads malware, the EDR system would prevent it from running, thereby neutralizing the threat. This provides a critical layer of defense after the user makes a mistake.

This approach directly mitigates risk by containing the potential damage caused by a compromised endpoint. EDR systems can also detect and isolate infected machines, preventing lateral movement within the network. This proactive intervention is more effective at damage control than solely relying on user awareness or email filtering.

Further Research:

NIST SP 800-207 Zero Trust Architecture:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (Provides a framework that aligns with minimizing the blast radius of security incidents)
SANS Institute Endpoint Detection and Response (EDR):https://www.sans.org/reading-room/whitepapers/endpoint/endpoint-detection-response-edr-36267 (Explains the functionalities and benefits of EDR systems.)

Question: 66

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A.Compensating control
B.Network segmentation
C.Transfer of risk
D.SNMP traps

Answer: A

Explanation:

The correct answer is A. Compensating Control. Here's why:

A compensating control is a security measure implemented to mitigate risk when a primary security control is either not feasible or not fully effective. In the scenario, the legacy Linux system lacks modern security features or patching capabilities. Thus, directly securing the system is problematic.

The host-based firewall, configured to only allow connections from specific internal IP addresses, is acting as a compensating control. It is not ideal (network segmentation would be preferable), but it reduces the attack surface and limits the impact of a potential compromise. Instead of a full-blown network segmentation (Option B), which would involve dedicated network hardware and configurations, the firewall is used to "compensate" for the system's inherent vulnerabilities.

Transfer of risk (Option C) involves shifting the risk to another party, such as through insurance. SNMP traps (Option D) are network management alerts and irrelevant to limiting access.

The host-based firewall provides an alternative security measure, making A the most fitting answer. It doesn't

MYEXAM.FR

remove the risk entirely (like network segmentation ideally would), but it significantly decreases it due to inherent limitations.Reference:

NIST Special Publication 800-53 (See discussion on Control Enhancements and Compensating Controls)

Question: 67

The management team notices that new accounts that are set up manually do not always have correct access or permissions.
Which of the following automation techniques should a systems administrator use to streamline account creation?

A.Guard rail script

B.Ticketing workflow

C.Escalation script

D.User provisioning script

Answer: D

Explanation:

The correct answer is **D. User provisioning script**. Here's why:

The scenario describes inconsistent account configurations when created manually, leading to incorrect access and permissions. User provisioning scripts directly address this problem by automating the account creation process. A user provisioning script is a set of instructions that automatically configures new user accounts with the correct roles, permissions, and access rights, ensuring consistency and reducing errors inherent in manual processes. This automation eliminates the variability introduced by human error, ensuring all new accounts adhere to predefined security policies. The script can integrate with identity and access management (IAM) systems, directory services (like Active Directory or LDAP), and other relevant systems to manage user accounts centrally. It can be triggered by HR systems upon employee onboarding or via self-service portals.

A guard rail script (A) helps maintain compliance and prevents actions that violate security policies within an existing environment, but it doesn't automate the initial account creation. A ticketing workflow (B) automates the process of requesting and approving account creation, but it doesn't automate the technical configuration of the account itself. An escalation script (C) automates the notification and transfer of an issue to a higher support level when certain conditions are met. Thus, only user provisioning script directly addresses the automation of user account creation with appropriate roles and permissions.

Further Research:

NIST Special Publication 800-63-3 (Digital Identity Guidelines):https://pages.nist.gov/800-63-3/
Microsoft's Active Directory User Provisioning:https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning

MYEXAM.FR

Question: 68

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

A.Corrective

B.Preventive

C.Detective

D.Deterrent

Answer: C

Explanation:

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

A detective control aims to identify and alert when a security incident has already occurred or is in progress. The SIEM system, in conjunction with the analyst reviewing the logs, is designed to detect suspicious activity or breaches that have bypassed preventive measures. The SIEM collects and analyzes logs from various systems, and the analyst's review acts as the human component to identify anomalies indicating a security issue.

A corrective control (A) would be implemented to fix or restore systems after an incident has occurred. Examples include restoring from backups or patching vulnerabilities. A preventive control (B) aims to stop incidents from happening in the first place, such as firewalls, intrusion prevention systems (IPS), and access controls. A deterrent control (D) aims to discourage potential attackers, like security cameras or warning signs.

The scenario describes the company's effort to identify security incidents through log analysis, which aligns perfectly with the definition of a detective control. The weekly review schedule emphasizes that the purpose is to discover past or ongoing events, not to prevent them proactively.

For further information on security controls, refer to resources from organizations like NIST (National Institute of Standards and Technology):

NIST Special Publication 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final SANS Institute: https://www.sans.org/

MYEXAM.FR

Question: 69

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

A.Serverless framework

B.Type 1 hypervisor

C.SD-WAN

D.SDN

Answer: A

Explanation:

The question asks for a low-cost, cloud-based application hosting solution. Serverless frameworks are the most appropriate choice because they offer a pay-as-you-go model, meaning you only pay for the compute time your application consumes. This can significantly reduce costs compared to traditional server-based hosting where you pay for the server regardless of utilization. Serverless architectures abstract away the underlying infrastructure management, freeing the administrator from managing servers, patching operating systems, and scaling resources. This operational efficiency can translate to further cost savings.

Type 1 hypervisors are bare-metal hypervisors that run directly on the hardware and are typically used for virtualization within an on-premises environment or private cloud; they are not directly application hosting solutions in the public cloud sense and do not necessarily offer cost advantages depending on the overall infrastructure setup. SD-WAN (Software-Defined Wide Area Network) is a networking technology used to manage and optimize network traffic across a wide area network, it focuses on connectivity rather than application hosting. SDN (Software-Defined Networking) is a networking architecture focusing on centrally managing network resources; also, it does not directly address application hosting requirements or cost considerations.

Serverless computing perfectly fits the cloud-based, low-cost requirement by automatically scaling resources based on application demand and charging only for the actual resources consumed.

For further research, consider the following links:

AWS Lambda: https://aws.amazon.com/lambda/
Azure Functions: https://azure.microsoft.com/en-us/products/functions
Google Cloud Functions: https://cloud.google.com/functions

These services are excellent examples of serverless platforms.

Question: 70

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A.Tuning
B.Aggregating
C.Quarantining
D.Archiving

Answer: A

Explanation:

The correct answer is **A. Tuning**. Tuning, in the context of security monitoring and incident response, involves adjusting security tools and systems to reduce false positives and false negatives. The scenario describes a situation where an initial alert flagged activity as malicious, but further investigation determined it was normal. Therefore, to prevent similar alerts from triggering in the future for the same normal activity, the system needs to be adjusted. This adjustment is called tuning.

Tuning can involve modifying rules, thresholds, or whitelists within security information and event management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS), or other security tools. By tuning the system, the SOC is effectively teaching it to recognize the previously flagged activity as benign. This reduces alert fatigue and allows analysts to focus on genuine threats. Failing to tune the system would result in repeated alerts for the same normal activity, overwhelming analysts and potentially obscuring real threats.

Aggregating (B) combines multiple logs or events into a single, more comprehensive record but doesn't address the problem of repeated false positives. Quarantining (C) isolates a potentially infected system, which is not appropriate when the activity is deemed normal. Archiving (D) stores data for long-term retention and doesn't affect real-time alerting. Thus, only tuning specifically addresses the need to suppress future alerts for activity determined to be normal.

For further reading, explore SIEM best practices and tuning strategies, such as those outlined by SANS Institute or NIST guidelines on security incident handling. These resources emphasize the importance of continuous monitoring and adjustment of security tools to maintain effectiveness.

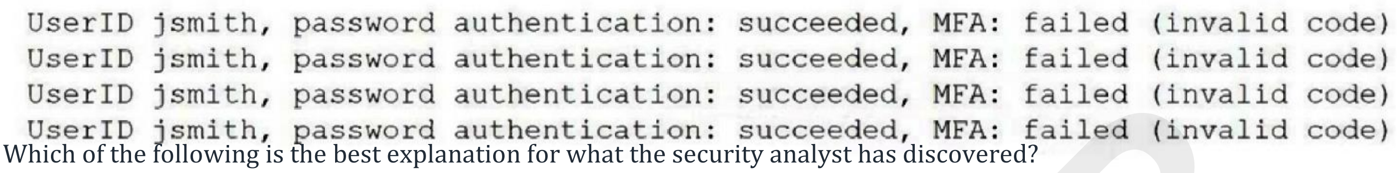
SANS Institute:https://www.sans.org/ (Search for articles on SIEM tuning and incident response)

MYEXAM.FR

NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 71

A security analyst reviews domain activity logs and notices the following:



```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A.The user jsmith’s account has been locked out.

B.A keylogger is installed on jsmith’s workstation.

C.An attacker is attempting to brute force jsmith’s account.

D.Ransomware has been deployed in the domain.

Answer: C

Explanation:

An attacker is attempting to brute force jsmith’s account.

Question: 72

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A.Clustering servers

B.Geographic dispersion

C.Load balancers

D.Off-site backups

Answer: B

Explanation:

The correct answer is **B. Geographic dispersion.**

Here's a detailed justification:

Geographic dispersion refers to strategically distributing IT infrastructure across multiple geographically separated locations. This approach is vital for mitigating risks associated with localized disasters such as weather events, power outages, or regional cyberattacks. If a server room in one location is affected by a hurricane, flood, or earthquake, the other geographically dispersed locations can continue to operate, ensuring business continuity and minimizing downtime.

Clustering servers (A) enhances availability and performance by grouping multiple servers to work as a single system. While it provides redundancy within a single location or a limited area, it doesn't protect against a disaster that affects that entire location. Load balancers (C) distribute network traffic across multiple servers, also mainly improving performance and availability within a specific site, not across geographically diverse sites. Off-site backups (D) are essential for data recovery in the event of a complete system failure, but they

MYEXAM.FR

do not provide immediate failover capabilities and require time to restore, leading to downtime. Geographic dispersion, in contrast, provides a near-instantaneous switchover to a functioning site in case of a disaster at the primary site. It offers higher availability and resilience than simply having off-site backups. The geographically dispersed sites can actively serve users, rather than just holding data for restoration.

In the context of cloud computing, geographic dispersion is often achieved through multi-region or multi-availability zone deployments. Cloud providers like AWS, Azure, and GCP offer services that allow organizations to replicate their infrastructure and data across different regions, providing a robust solution for disaster recovery and business continuity. By using these services, companies can ensure that their applications and data remain available even if one region experiences an outage.

Further reading:

AWS Global Infrastructure:https://aws.amazon.com/about-aws/global-infrastructure/
Azure Regions:https://azure.microsoft.com/en-us/global-infrastructure/regions/ **Google Cloud Regions:**https://cloud.google.com/about/locations

Question: 73

Which of the following is a primary security concern for a company setting up a BYOD program?

A.End of life
B.Buffer overflow
C.VM escape
D.Jailbreaking

Answer: D

Explanation:

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

BYOD (Bring Your Own Device) programs introduce unique security challenges. While options A, B, and C are valid security concerns in general IT environments, jailbreaking poses the most immediate and direct risk within a BYOD context.

Jailbreaking/Rooting: This process bypasses the operating system's built-in security restrictions on iOS (jailbreaking) and Android (rooting) devices. While users may do this for customization or to install unofficial apps, it significantly weakens the device's security posture. This can lead to easier malware infection, data leakage, and unauthorized access to company resources. Jailbroken devices often lack standard security updates, leaving them vulnerable to known exploits. Company security policies and mobile device management (MDM) solutions become ineffective on such devices. The circumvention of security controls is the main reason behind this concern.

End-of-Life: While EOL devices present vulnerabilities due to lack of updates, a BYOD policy should actively discourage and ultimately exclude devices that no longer receive security patches. This is an important policy enforcement issue, but is addressable through documented acceptance of the risk or proactive device retirement.

Buffer Overflow: A buffer overflow is a programming error that can be exploited to run malicious code. While concerning, it is not a direct issue arising specifically from BYOD. This is a more general software vulnerability.

VM Escape: VM escape allows an attacker to break out of a virtual machine and access the host system or other VMs on the same host. This is highly relevant in cloud computing and virtualization environments but is less directly related to the risks introduced by end-user devices in a BYOD program.

MYEXAM.FR

Therefore, the primary security concern with BYOD is the potential for users to jailbreak or root their devices, circumventing security controls and increasing the risk of malware and data breaches.

For further reading, refer to:

NIST Guidelines on BYOD: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-124r1.pdf SANS Institute on BYOD Security: https://www.sans.org/white-papers/33397/

Question: 74

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.
Which of the following analysis elements did the company most likely use in making this decision?

A.MTTR
B.RTO
C.ARO
D.MTBF

Answer: C

Explanation:

The correct answer is **C. ARO (Annualized Rate of Occurrence)**. Here's why:

The company's decision to drop ransomware coverage likely stemmed from an analysis of the potential financial impact of ransomware attacks versus the cost of the insurance premium. ARO is a key component of quantitative risk assessment.

ARO represents the estimated frequency of a threat event (in this case, a ransomware attack) occurring in a single year. By estimating the ARO of ransomware attacks and combining this with the potential financial loss (Single Loss Expectancy or SLE) if an attack were to occur, the company could calculate the Annualized Loss Expectancy (ALE). (ALE = SLE x ARO)

If the ALE (the projected annual loss from ransomware) was lower than the cost of the insurance premium, the company might rationally decide that self-insuring (i.e., bearing the risk themselves) was more cost-effective. This means they judged the likelihood of a ransomware attack (ARO) and its associated financial impact (SLE) as not justifying the expense of insurance.

MTTR (Mean Time to Repair) refers to the average time it takes to restore a system or service after a failure. While important for incident response, it doesn't directly influence the decision of whether to carry ransomware insurance.

RTO (Recovery Time Objective) is the target time within which a business process should be restored after a disruption. Like MTTR, RTO is about incident recovery, not risk assessment for insurance.

MTBF (Mean Time Between Failures) predicts the average time between failures of a system. This is useful for reliability analysis, but less relevant for assessing the risk and cost of a specific event like a ransomware attack for insurance purposes.

In essence, the company weighed the probable annual cost of ransomware incidents (based on ARO and SLE) against the insurance premium and decided the risk didn't warrant the coverage. The assessment of the frequency of the threat, represented by ARO, was central to that determination.

Further Research:

MYEXAM.FR

NIST Risk Management Framework:https://csrc.nist.gov/projects/risk-management - This framework provides detailed guidance on risk assessment methodologies.

SANS Institute:https://www.sans.org/ - SANS offers various resources and courses on risk assessment and cybersecurity. Specifically, look for materials on quantitative risk assessment.

Question: 75

Which of the following is the most likely to be included as an element of communication in a security awareness program?

A.Reporting phishing attempts or other suspicious activities

B.Detecting insider threats using anomalous behavior recognition

C.Verifying information when modifying wire transfer data

D.Performing social engineering as part of third-party penetration testing

Answer: A

Explanation:

The correct answer is **A. Reporting phishing attempts or other suspicious activities.**

Here's a detailed justification:

A security awareness program aims to educate employees about cybersecurity threats and best practices to mitigate risks. Effective communication is crucial for its success. The core purpose of such a program is to modify employee behavior, making them an active part of the organization's defense.

Option A directly relates to empowering employees to identify and report potential threats. Reporting phishing attempts or suspicious activities is a fundamental element of a security awareness program because it leverages the "human firewall." Employees are often the first line of defense against phishing attacks and other social engineering tactics. By training them to recognize these threats and providing a clear reporting mechanism, organizations can significantly reduce their exposure to risk. Reporting suspicious activity enables security teams to analyze trends, identify emerging threats, and respond proactively. It also reinforces a security-conscious culture where employees feel responsible for protecting organizational assets.

Option B, detecting insider threats using anomalous behavior recognition, is a more technical aspect, often handled by dedicated security tools and teams, rather than being a primary communication objective of a security awareness program. While the awareness program might mention insider threats, the detection itself relies on sophisticated technologies and analysts.

Option C, verifying information when modifying wire transfer data, is a specific security control related to financial transactions. While important, it's a targeted procedural control, rather than a broad communication element of the entire security awareness program. It falls under the broader topic of financial security awareness but isn't the most likely core element.

Option D, performing social engineering as part of third-party penetration testing, is a security assessment activity, not a communication element aimed at employees within the context of a security awareness program. While employees might be informed that such testing may occur, the performance is an external exercise.

Therefore, communicating the importance and process of reporting phishing and other suspicious activities is a foundational and universally applicable element of any security awareness program, making it the most likely answer.

MYEXAM.FR

Further reading:

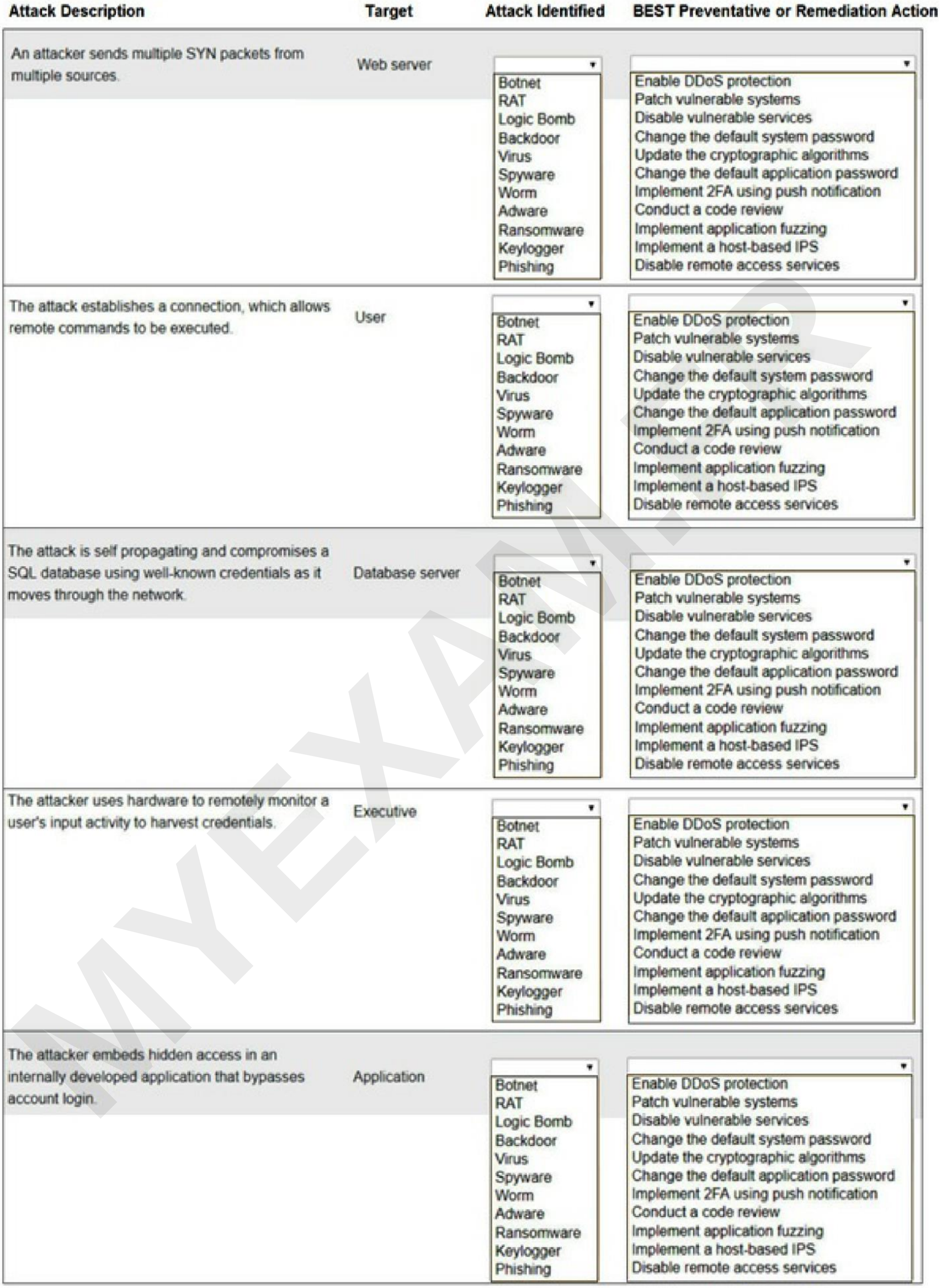
SANS Institute on Security Awareness: https://www.sans.org/information-security-topics/security-awareness/
NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program: https://csrc.nist.gov/publications/detail/sp/800-50/archive/2003-08-01

Question: 76

HOTSPOT -
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

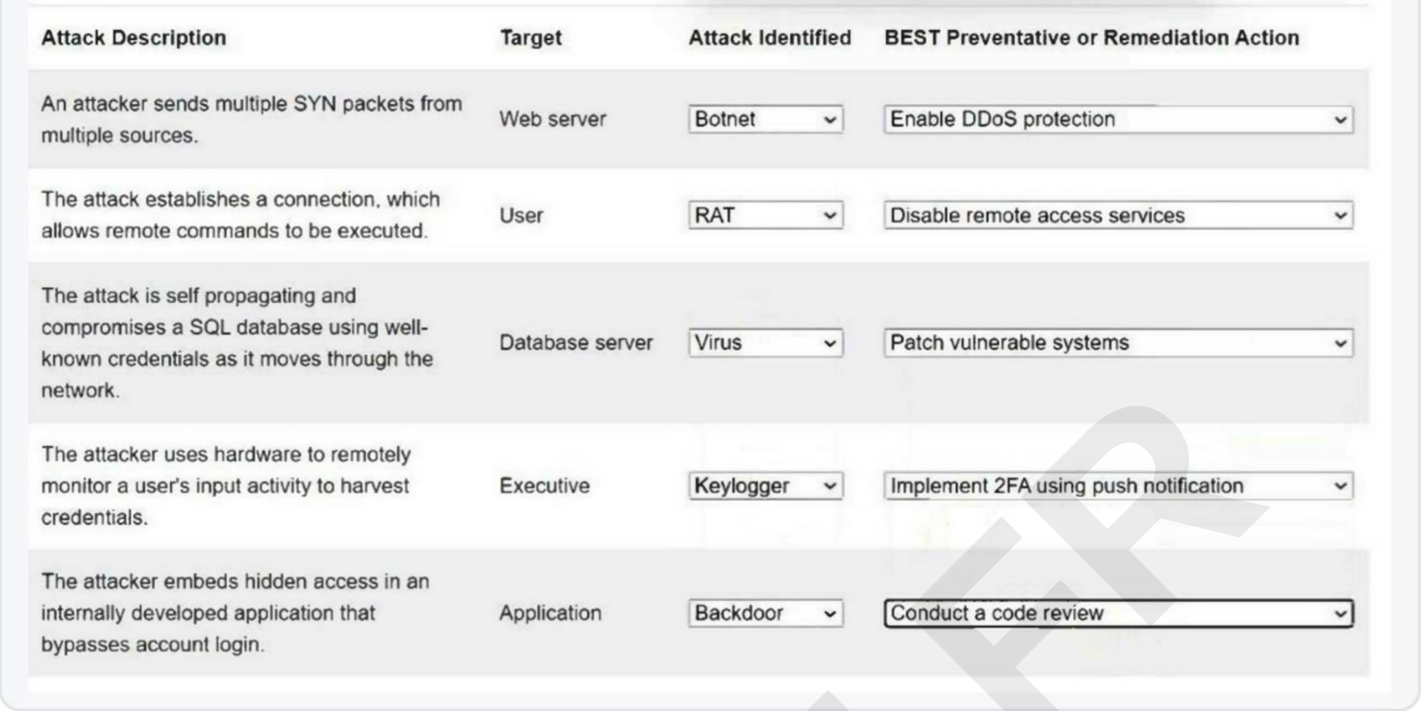
MYEXAM.FR



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

MYEXAM.FR

Answer:



Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Virus	Patch vulnerable systems
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

EXAM.FR

Question: 77

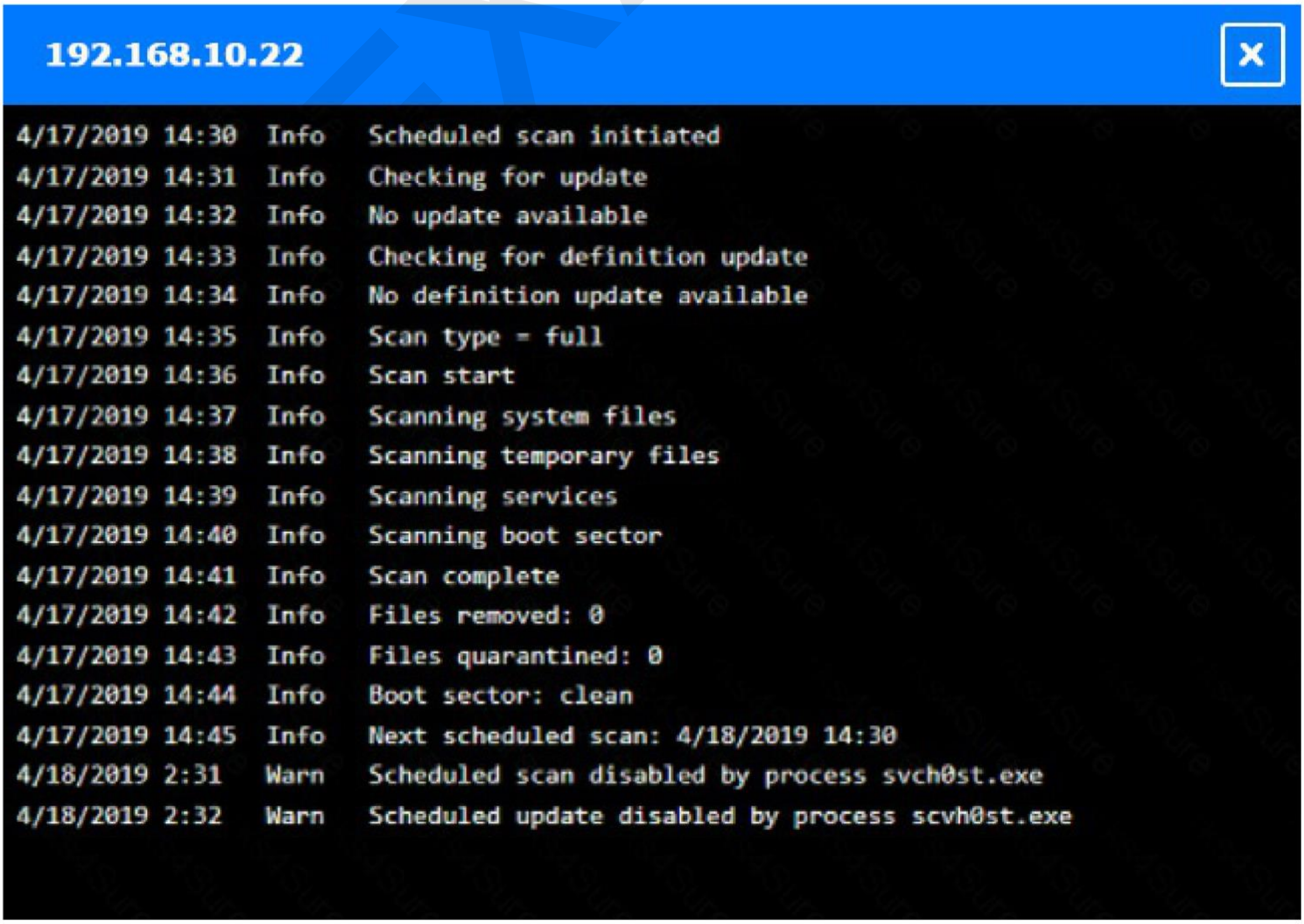
HOTSPOT -

You are a security administrator investigating a potential infection on a network.

INSTRUCTIONS -

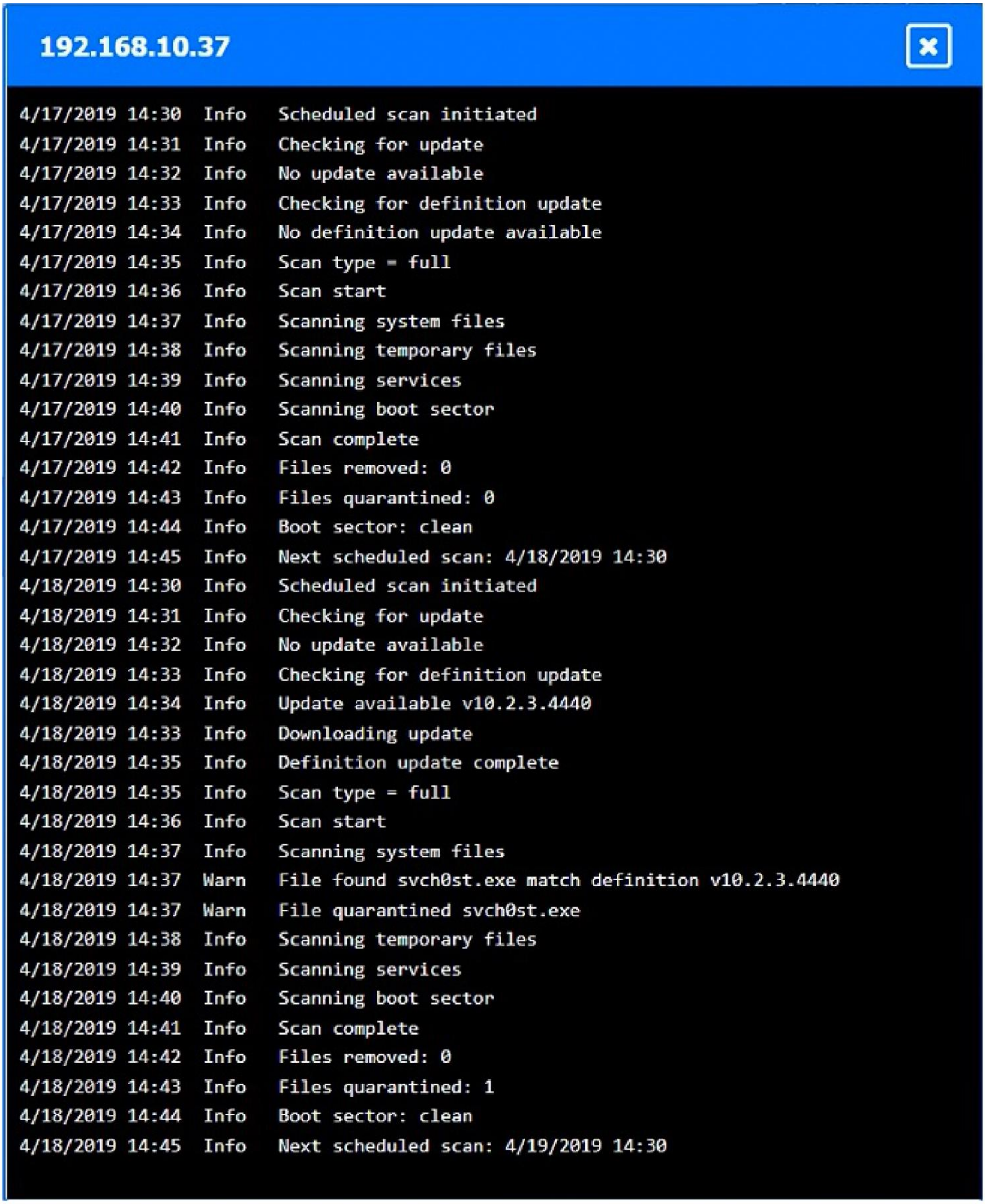
Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

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



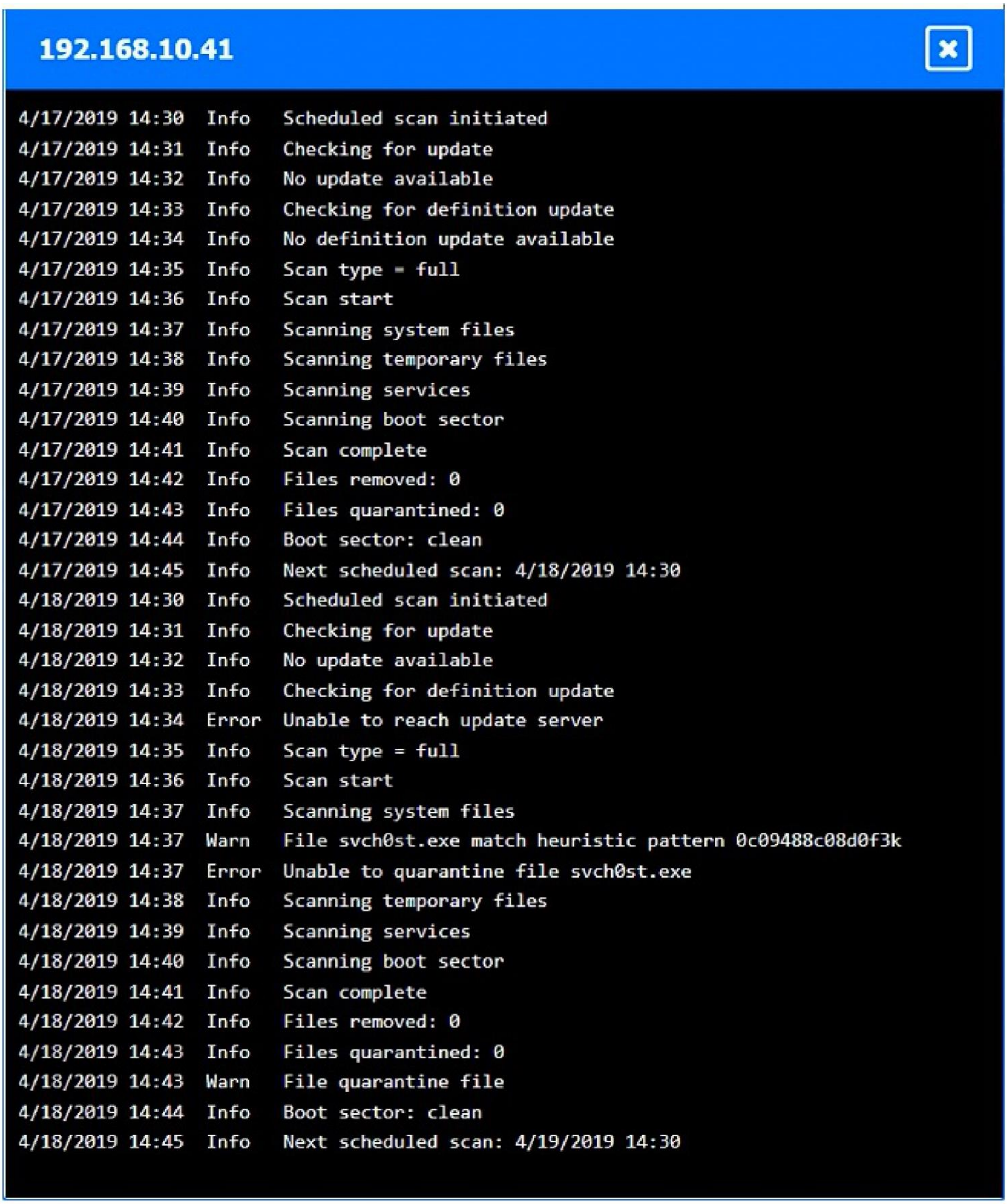
192.168.10.22

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31   Warn   Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32   Warn   Scheduled update disabled by process scvh0st.exe
```



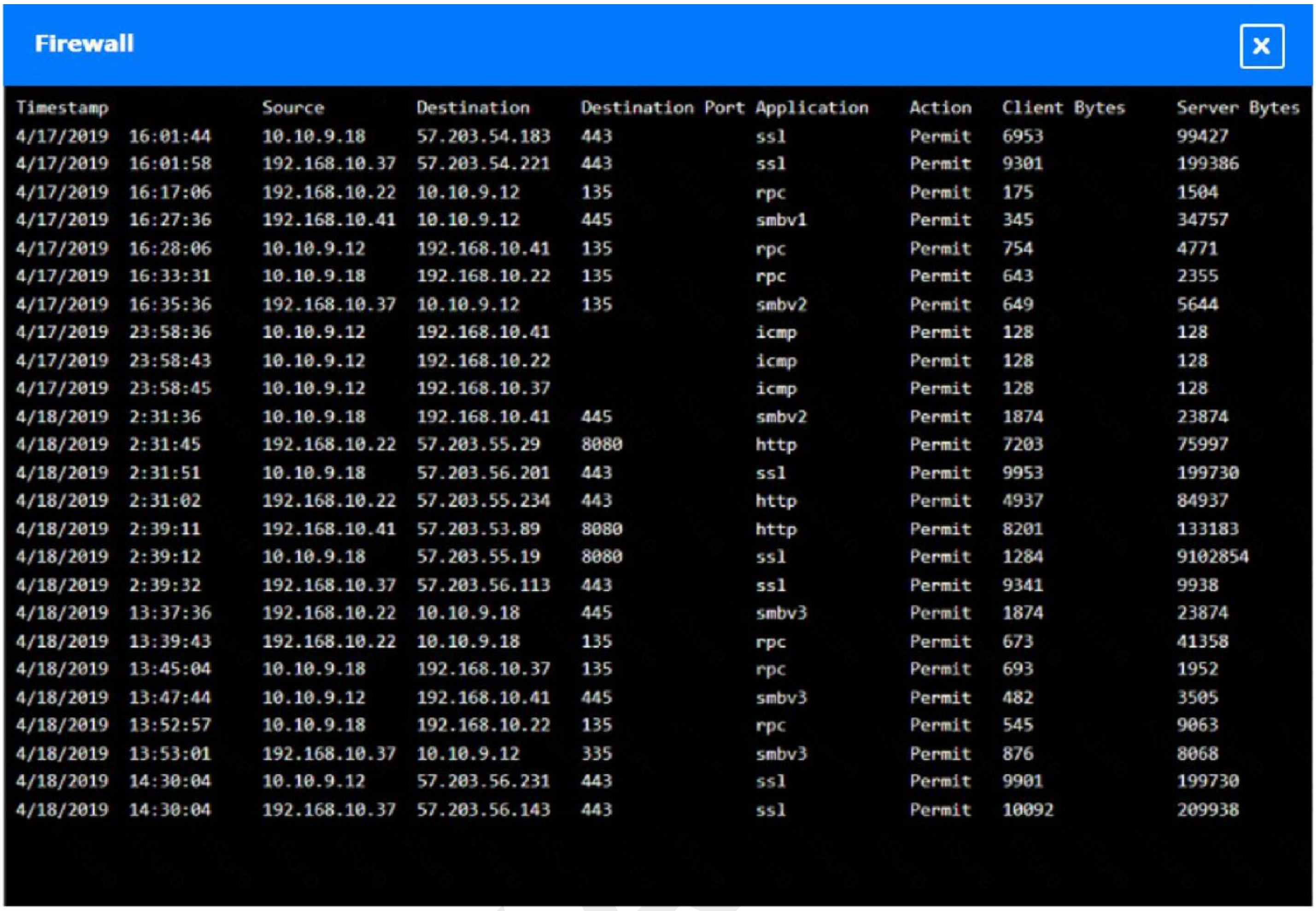
192.168.10.37

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 1
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



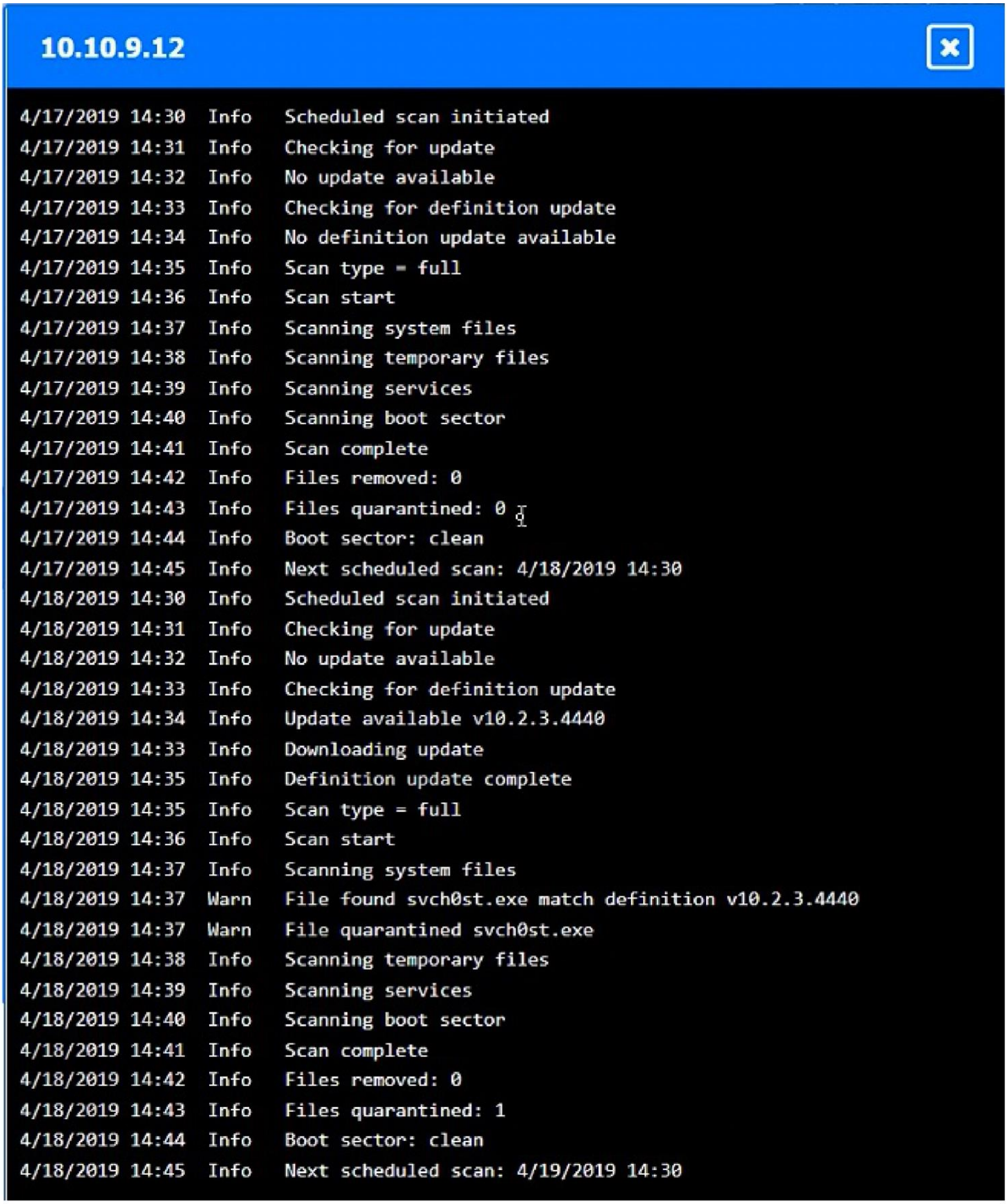
192.168.10.41

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



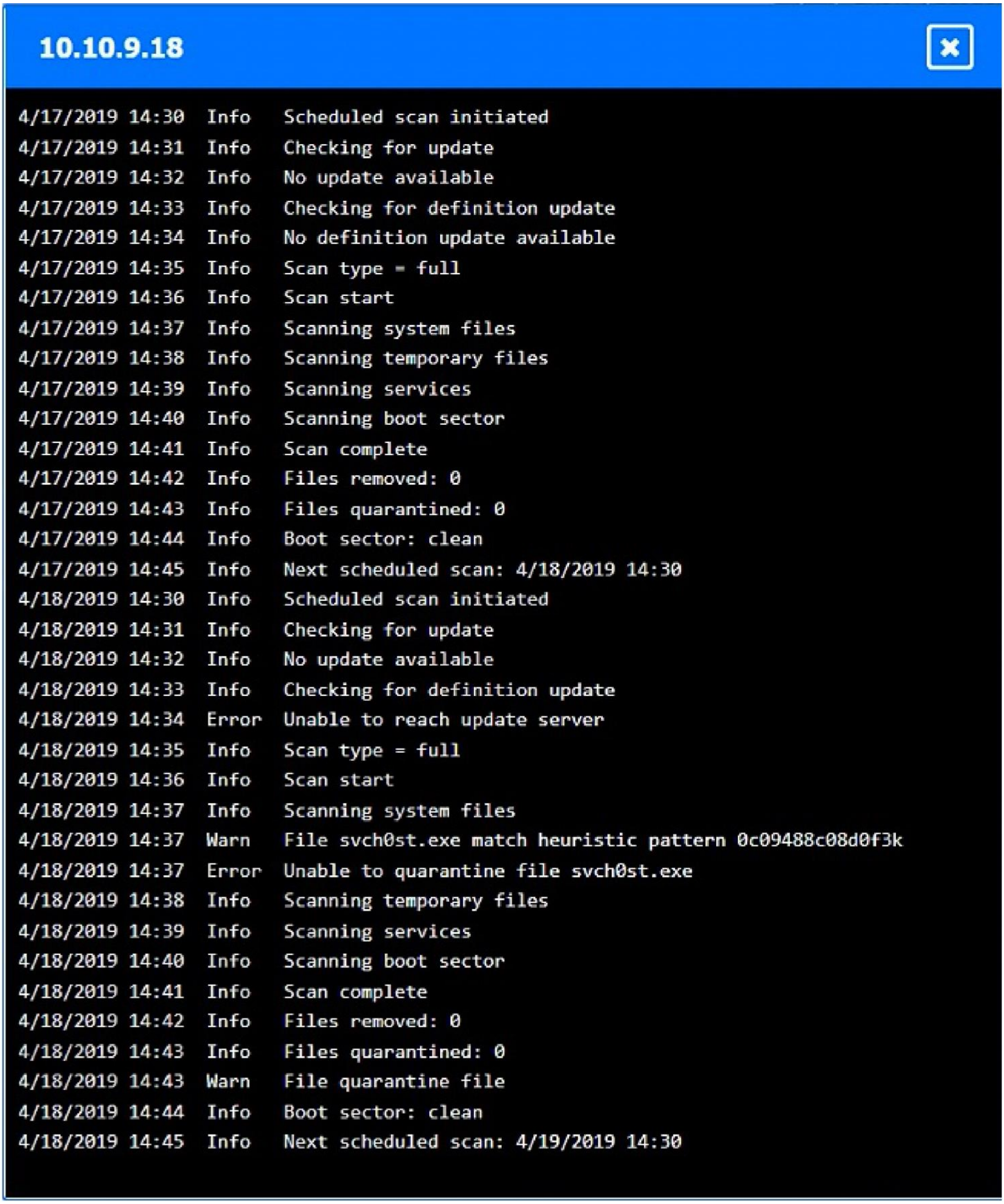
```
Timestamp           Source         Destination    Destination Port Application  Action  Client Bytes    Server Bytes
4/17/2019  16:01:44 10.10.9.18     57.203.54.183  443              ssl          Permit  6953            99427
4/17/2019  16:01:58 192.168.10.37  57.203.54.221  443              ssl          Permit  9301            199386
4/17/2019  16:17:06 192.168.10.22  10.10.9.12     135              rpc          Permit  175             1504
4/17/2019  16:27:36 192.168.10.41  10.10.9.12     445              smbv1        Permit  345             34757
4/17/2019  16:28:06 10.10.9.12     192.168.10.41  135              rpc          Permit  754             4771
4/17/2019  16:33:31 10.10.9.18     192.168.10.22  135              rpc          Permit  643             2355
4/17/2019  16:35:36 192.168.10.37  10.10.9.12     135              smbv2        Permit  649             5644
4/17/2019  23:58:36 10.10.9.12     192.168.10.41                   icmp         Permit  128             128
4/17/2019  23:58:43 10.10.9.12     192.168.10.22                   icmp         Permit  128             128
4/17/2019  23:58:45 10.10.9.12     192.168.10.37                   icmp         Permit  128             128
4/18/2019  2:31:36  10.10.9.18     192.168.10.41  445              smbv2        Permit  1874            23874
4/18/2019  2:31:45  192.168.10.22  57.203.55.29   8080             http         Permit  7203            75997
4/18/2019  2:31:51  10.10.9.18     57.203.56.201  443              ssl          Permit  9953            199730
4/18/2019  2:31:02  192.168.10.22  57.203.55.234  443              http         Permit  4937            84937
4/18/2019  2:39:11  192.168.10.41  57.203.53.89   8080             http         Permit  8201            133183
4/18/2019  2:39:12  10.10.9.18     57.203.55.19   8080             ssl          Permit  1284            9102854
4/18/2019  2:39:32  192.168.10.37  57.203.56.113  443              ssl          Permit  9341            9938
4/18/2019  13:37:36 192.168.10.22  10.10.9.18     445              smbv3        Permit  1874            23874
4/18/2019  13:39:43 192.168.10.22  10.10.9.18     135              rpc          Permit  673             41358
4/18/2019  13:45:04 10.10.9.18     192.168.10.37  135              rpc          Permit  693             1952
4/18/2019  13:47:44 10.10.9.12     192.168.10.41  445              smbv3        Permit  482             3505
4/18/2019  13:52:57 10.10.9.18     192.168.10.22  135              rpc          Permit  545             9063
4/18/2019  13:53:01 192.168.10.37  10.10.9.12     335              smbv3        Permit  876             8068
4/18/2019  14:30:04 10.10.9.12     57.203.56.231  443              ssl          Permit  9901            199730
4/18/2019  14:30:04 192.168.10.37  57.203.56.143  443              ssl          Permit  10092           209938
```

MYEXA



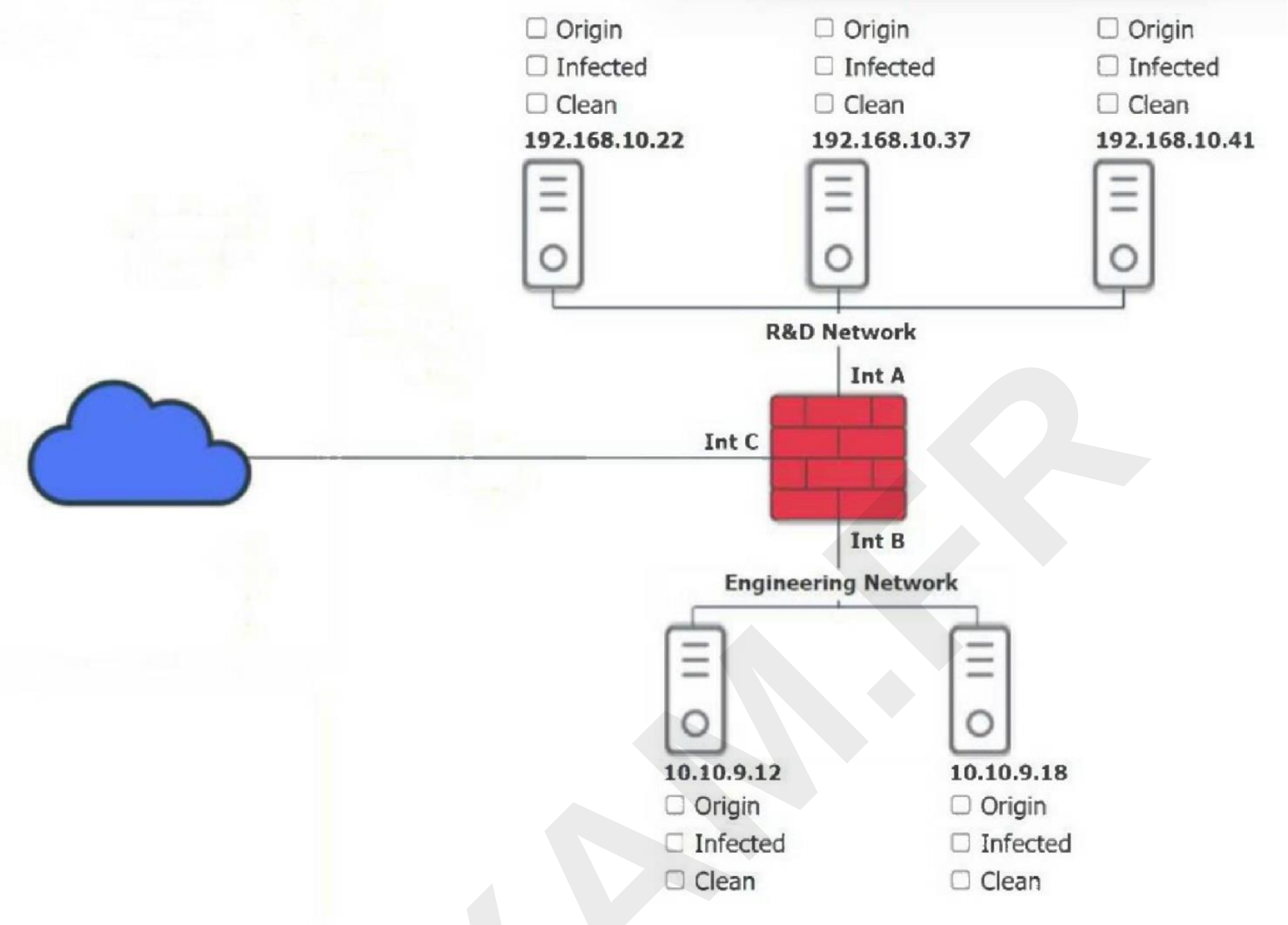
10.10.9.12

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 1
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



10.10.9.18

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



192.168.10.22
□ Origin
□ Infected
□ Clean

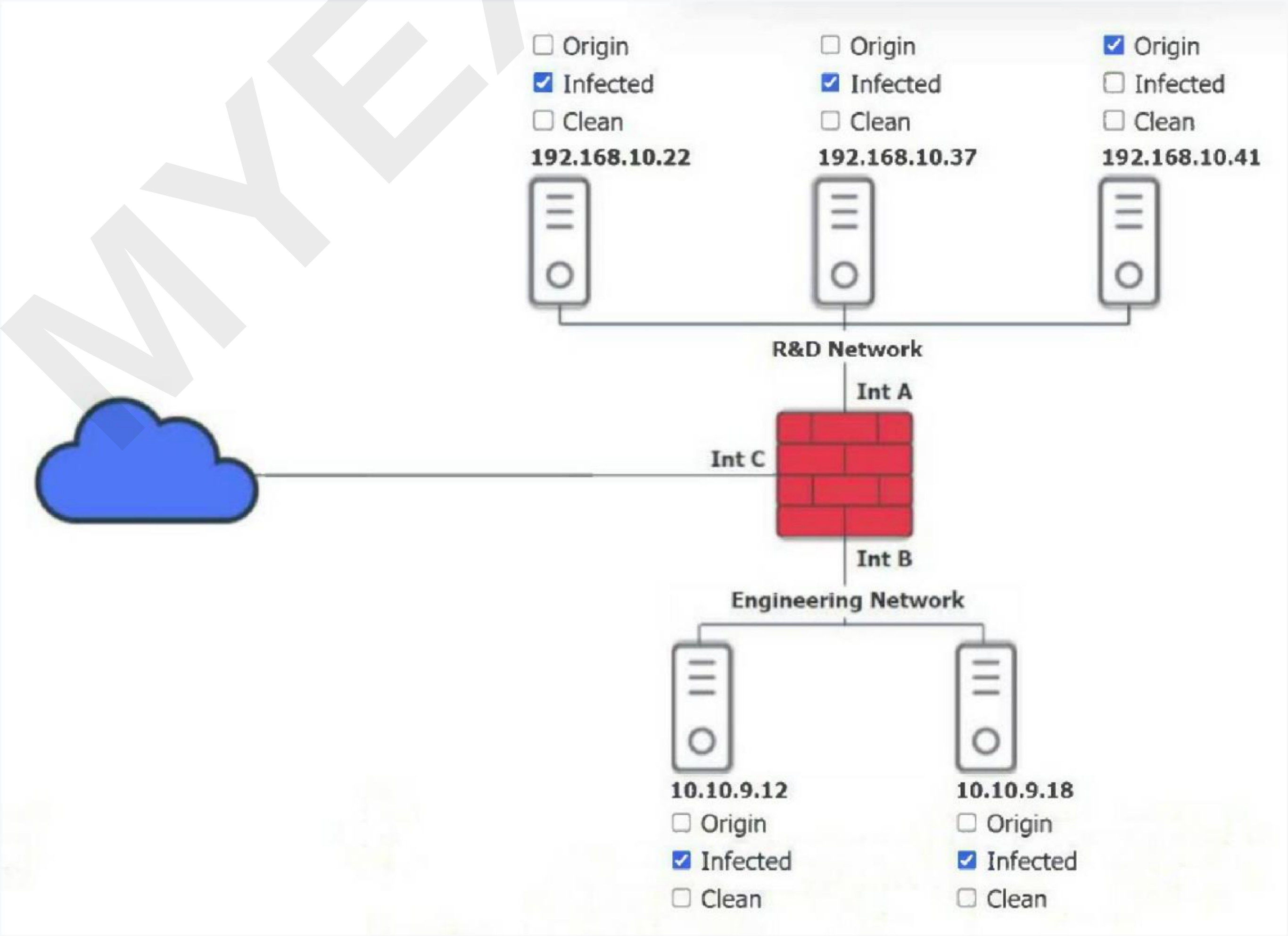
192.168.10.37
□ Origin
□ Infected
□ Clean

192.168.10.41
□ Origin
□ Infected
□ Clean

10.10.9.12
□ Origin
□ Infected
□ Clean

10.10.9.18
□ Origin
□ Infected
□ Clean

Answer:



192.168.10.22
□ Origin
☑ Infected
□ Clean

192.168.10.37
□ Origin
☑ Infected
□ Clean

192.168.10.41
☑ Origin
□ Infected
□ Clean

10.10.9.12
□ Origin
☑ Infected
□ Clean

10.10.9.18
□ Origin
☑ Infected
□ Clean

MYEXAM.FR

Question: 78

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A.Preparation

B.Recovery

C.Lessons learned

D.Analysis

Answer: A

Explanation:

The correct answer is A. Preparation.

The incident response process encompasses several phases designed to effectively manage and mitigate security incidents. The preparation phase is the first and arguably most crucial phase, as it lays the groundwork for a successful incident response. This phase involves establishing policies, procedures, and resources required to handle incidents efficiently. A key element of preparation is defining and documenting roles and responsibilities for incident response team members. This ensures that everyone understands their tasks and obligations during an incident.

Reviewing roles and responsibilities during preparation allows for clarification of who is responsible for specific actions, communication protocols, escalation paths, and decision-making authority. This proactive approach avoids confusion and delays when an actual incident occurs. For example, the designated incident commander, communication lead, and technical analysts should know their responsibilities beforehand.

Recovery focuses on restoring systems and services to normal operation after an incident, lessons learned analyzes the incident to improve future responses, and analysis investigates the incident to understand its scope and impact. While roles might be reinforced or refined during these later phases, the initial definition and review take place during preparation. Therefore, preparation is the phase where roles and responsibilities are explicitly reviewed and established to ensure a well-organized and effective response to security incidents.

Authoritative links:

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/

MYEXAMER

Question: 79

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A.Console access

B.Routing protocols

C.VLANs

D.Web-based administration

Answer: D

Explanation:

Web-based administration (option D) is the most appropriate feature to disable when hardening routers due to its inherent security risks. Web-based interfaces, while convenient, are often vulnerable to various web-based attacks such as cross-site scripting (XSS), cross-site request forgery (CSRF), and brute-force attacks targeting login credentials. These attacks can provide unauthorized access to the router's configuration, potentially leading to network compromise.

Disabling web-based access forces administrators to use more secure methods like SSH (Secure Shell) or console access for configuration changes. SSH provides an encrypted connection, significantly mitigating the risk of eavesdropping and man-in-the-middle attacks. Console access, which requires physical proximity, further reduces the attack surface.

Disabling console access (option A) would severely hinder legitimate administrative tasks and troubleshooting, making the router difficult to manage. Routing protocols (option B) are essential for the core functionality of routers, enabling them to forward traffic efficiently across the network; disabling them would cripple network connectivity. VLANs (option C) are used for network segmentation and security, and disabling them would reduce the network's overall security posture. Therefore, these options are less desirable from a security and operational perspective than disabling web-based administration. Reducing the attack surface is a primary security hardening strategy.

Further Reading:

SANS Institute on Router Security: https://www.sans.org/reading-room/whitepapers/networkdevices/securing-router-366
NIST Guide to Enterprise Patch Management Technologies: https://csrc.nist.gov/publications/detail/sp/800-40/ver-3/final (While about patch management, NIST publications often contain broad security hardening advice.)

Question: 80

A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

A.SPF
B.GPO
C.NAC
D.FIM

Answer: D

Explanation:

The answer is D, FIM (File Integrity Monitoring), because it's the most appropriate security control for tracking changes to data.

File Integrity Monitoring (FIM) is a security process that validates the integrity of operating system, application software files, and data files by using a checksum, hash or other cryptographic method. The computed value is stored and periodically compared against current values. Any differences between the stored value and the current value indicate that the file has been altered, which could be the result of an authorized change, a malicious attack, or an error. FIM systems typically generate alerts or reports when unauthorized changes are detected, enabling administrators to investigate and respond to potential security incidents. SPFB (Static Program Function Branching) is not a known security term. GPO (Group Policy Object) is a feature in Windows environments to control the working environment of user and computer accounts, but

MYEXAM.FR

does not necessarily provide integrity checks for files. NAC (Network Access Control) is a security solution that controls access to a network based on various factors, but it doesn't directly monitor file integrity. FIM directly addresses the requirement of securing data with change tracking.

For further research:

SANS Institute on FIM:https://www.sans.org/information-security/glossary/file-integrity-monitoring **NIST Guide to Intrusion Detection and Prevention Systems (IDPS):** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (While focusing on IDPS, it discusses integrity checking methodologies)

MYEXAM.FR

MYEXAM.FR