**Exam Topic Breakdown**

| Exam Topic | Number of Questions |
|---|---|
| Topic 1 : Exam Set 1 | 180 |
| Topic 2 : Exam Set 2 | 182 |
| Topic 3 : Exam Set 3 | 111 |
| Topic 4 : Exam Set 4 | 75 |
| TOTAL | 548 |

Question #:26 - (Exam Topic 4)

When implementing automation with loT devices, which of the following should be considered first to keep the network secure?

A. Z-Wave compatibility

B. Network range

C. Zigbee configuration

D. Communication protocols

**Answer: D**

**Explanation**

When implementing automation with IoT (Internet of Things) devices, the first consideration for network security should be the communication protocols used by these devices. IoT devices often use various communication protocols to interact with each other and the network, and the security of these protocols is crucial to ensure the overall security of the network.

Some common IoT communication protocols include Wi-Fi, Bluetooth, Zigbee, Z-Wave, and LoRaWAN. Each protocol has its own security features and vulnerabilities, and it is essential to choose protocols that have strong encryption, authentication mechanisms, and secure data transmission.

By prioritizing the security of communication protocols, network administrators can mitigate the risk of unauthorized access, data breaches, and other security incidents related to IoT devices in the network. Once secure communication protocols are established, other factors like Z-Wave compatibility, network range, and Zigbee configuration can be considered as additional security measures.

Question #:27 - (Exam Topic 4)

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

A. An employee receives a gift card request an email that has an executive's name the display held to 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 lo 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: A**

**Explanation**

An employee receiving a gift card request in an email that has an executive's name in the display field to the email describes a possible business email compromise attack. Business email compromise (BEC) is a type of phishing attack that targets employees who have access to financial or sensitive information, such as accounting, human resources, or executive staff. The attacker impersonates a trusted person, such as a manager, vendor, or client, and requests a fraudulent payment, wire transfer, gift card purchase, or personal information. The attacker may spoof the email address or display name, use a look-alike domain, or compromise a legitimate email account to make the request seem authentic.

Reference: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

Question #:28 - (Exam Topic 4)

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks. Which of the following would be best for the security manager to use in a threat model?

A. Hacktivists

B. White-hat hackers

C. Script kiddies

D. Insider threats

**Answer: A**

**Explanation**

Hacktivists are hackers who use their skills to promote a political or social cause, such as human rights, environmentalism, anti-censorship, etc. Hacktivists may target organizations or individuals who oppose their views or agendas, and launch cyberattacks such as defacement, denial-of-service, data theft, or sabotage. In this case, the security manager should consider hacktivists as a potential threat actor who may launch cyberattacks in response to the CEO's controversial opinion article.

Question #:29 - (Exam Topic 4)

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

A. Geolocation

B. Time-of-day restrictions

C. Certificates

D. Tokens

E. Geotagging

F. Role-based access controls

**Answer: A B**

**Explanation**

Geolocation and time-of-day restrictions would be best to mitigate the CEO's concerns about staff members working from high-risk countries while on holiday or outsourcing work to a third-party organization in another country. Geolocation is a technique that involves determining the physical location of a device or user based on its IP address, GPS coordinates, Wi-Fi signals, or other indicators. Time-of-day restrictions are policies that limit the access or usage of resources based on the time of day or week. Geolocation and time-of-day restrictions can help to enforce access control rules, prevent unauthorized access, detect anomalous behavior, and comply with regulations. References: https://www.comptia.org/blog/what-is-geolocation

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Petra Martina Vrancic — Today at 10:08 AM

Tokens are often used in multi-factor authentication (MFA) systems to enhance authentication security. While MFA is crucial for securing access to company resources, it might not directly address concerns related to employees working from high-risk countries or outsourcing work.

can certainly be used in conjunction with these measures to enhance overall security, but they might not be the primary controls for addressing the CEO's specific concerns in this scenario. It's often effective to use a combination of security controls to create a robust and layered defense strategy.

Question #:30 - (Exam Topic 4)

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multi cloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

A. Trusted Platform Module

B. laaS

C. HSMaas ///////Hardware Security Module as a Service

D. PaaS

**Answer: C**

**Explanation**

HSMaas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption.
HSMaas allows the organization to use its own keys or generate new ones, and to control and manage them centrally

regardless of where the data is stored or processed. HSMaas also reduces the latency and complexity of managing multiple encryption keys across different cloud providers, as well as the cost and maintenance of deploying physical HSM devices.

A. Trusted Platform Module. This is not the correct answer, because a Trusted Platform Module (TPM) is a hardware chip that provides secure storage and generation of cryptographic keys on a device, such as a laptop or a server. A TPM does not offer a cloud-based solution for key management and encryption across multiple cloud providers.

B. laaS. This is not the correct answer, because laaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources, such as servers, storage, and networks, over the internet. laaS does not provide a specific solution for key management and encryption across multiple cloud providers.

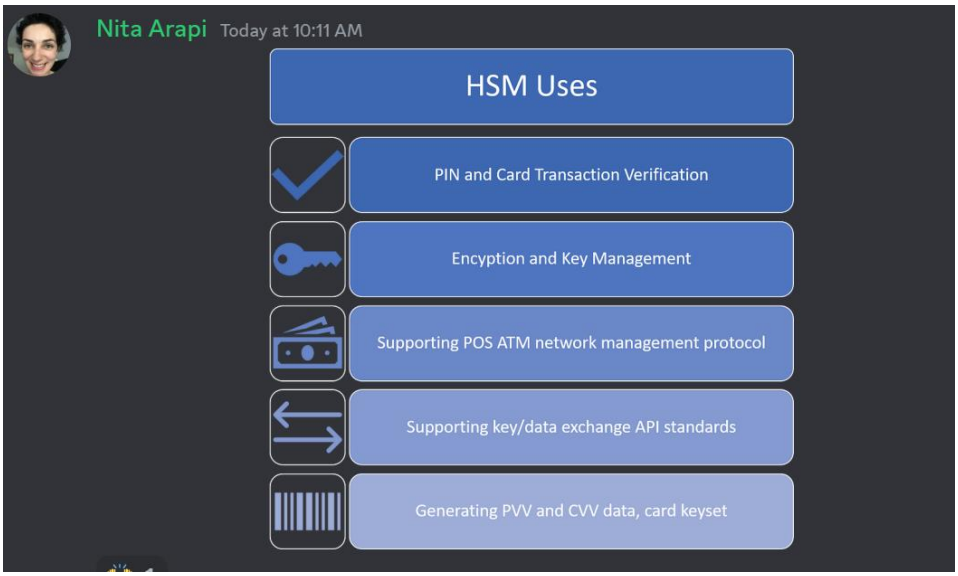
C. HSMaas. This is the correct answer, because HSMaas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption across multiple cloud providers.

D. PaaS. This is not the correct answer, because PaaS stands for Platform as a Service, which is a cloud computing model that provides a platform for developing and deploying applications over the internet. PaaS does not provide a specific solution for key management and encryption across multiple cloud providers.

Reference: HSM as a Service (HSMaaS) | Encryption Consulting, What Is Hardware Security Module (HSM)?

| Thales.

https://www.encryptionconsulting.com/what-is-hardware-security-module-as-a-service/




Question #:31 - (Exam Topic 4)

The most recent vulnerability scan flagged the domain controller with a critical vulnerability. The systems administrator researched the vulnerability and discovered the domain controller does not run the associated application with the vulnerability. Which of the following steps should the administrator take next?

A. Ensure the scan engine is configured correctly.

B. Apply a patch to the domain controller.

C. Research the CVE.

D. Document this as a false positive.

**Answer: D**

**Explanation**

A false positive is a result that indicates a problem when there is no actual problem. In this case, the vulnerability scan flagged the domain controller with a critical vulnerability, but the domain controller does not run the application that is vulnerable. Therefore, the scan result is inaccurate and should be documented as a false positive.

A. Ensure the scan engine is configured correctly. This is not the next step, because the scan engine may be configured correctly and still produce false positives due to various factors, such as outdated signatures, network latency, or misconfigured devices.

B. Apply a patch to the domain controller. This is not the next step, because applying a patch to a system that does not have the vulnerability may cause unnecessary problems or conflicts.

C. Research the CVE. This is not the next step, because the systems administrator already researched the vulnerability and discovered that it does not affect the domain controller.

D. Document this as a false positive. This is the correct answer, because documenting false positives helps to improve the accuracy and efficiency of future scans and audits.

Reference: CompTIA Security+ Study Guide (PDF) - Netwrix, page 14.

https://www.codecademy.com/article/vulnerability-scans

Question #:32 - (Exam Topic 4)

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker most likely use to gain access?

A. A bot

B. A fileless virus

C. A logic bomb

D. A RAT

**Answer: D**

**Explanation**

A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system without the user's knowledge or consent. A RAT can perform various malicious activities on the system, such as stealing data, installing other malware, deleting files, modifying settings, capturing keystrokes, recording audio or video, etc. In this case, the attacker most likely used a RAT to gain administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge

Reference: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/

Petra Martina Vrancic — Today at 10:16 AM

A bot typically refers to a botnet, and a logic bomb is a piece of code that triggers a malicious action under specific conditions. While both can be security threats

Question #:33 - (Exam Topic 4)

Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop

B. Replication

C. Failover

D. Recovery

**Answer: A**

**Explanation**

A tabletop exercise is a type of simulation exercise that involves discussing hypothetical scenarios and testing the incident response plan in a low-stress environment. A tabletop exercise can help an organization to improve its incident response process by identifying gaps, weaknesses, roles, responsibilities, communication channels, etc., and by evaluating the effectiveness and efficiency of the plan.

Reference: https://www.triaxiomsecurity.com/tips-to-improve-your-incident-response-tabletop-exercise/#:~:text=Practice%20Makes%20Perfect,end%2Dto%2Dend%20exercise.

Question #:34 - (Exam Topic 4)

Which of the following threat vectors would appear to be the most legitimate when used by a malicious actor to impersonate a company?

A. Phone call

B. Instant message

C. Email

D. Text message

**Answer: C**

**Explanation**

Email is one of the most common and effective threat vectors used by malicious actors to impersonate a company and conduct phishing or spear phishing attacks. Phishing is a type of social engineering attack where an attacker sends fraudulent emails that appear to be from a legitimate source, such as a company, a bank, a government agency, etc., and tries to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information. Email can appear to be more legitimate than other threat vectors because it can use spoofed sender addresses, logos, signatures, or domain names that resemble the real ones.

Reference: https://ciosea.economictimes.indiatimes.com/news/security/phishing-is-borderless-still-the-initial-vector-for-9-out-of-every-10-cyber-attacks-report/102717904#:~:text=2%20min%20read-,Phishing%20is%20borderless%2C%20still%20the%20initial%20vector%20for%209%20out,increasingly%20impersonating%20trusted%20name%20brands.

Question #:35 - (Exam Topic 4)

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:

The username you entered does not exist.

Which of the following should the analyst recommend be enabled?

A. Input validation

B. Obfuscation

C. Error handling

D. Username lockout

**Answer: C**

**Explanation**

Proper error handling would be most appropriate in this situation. The logon screen message that reveals the username does not exist is a security weakness that can help the attacker to guess valid usernames. A better message would be "Invalid username or password".

https://owasp.org/www-community/Improper_Error_Handling

Question #:36 - (Exam Topic 4)

Which of the following is an administrative control that would be most effective to reduce the occurrence of malware execution?

A. Security awareness training

B. Frequency of NIDS updates

C. Change control procedures

D. EDR reporting cycle

**Answer: A**

**Explanation**

Security awareness training is an administrative control that educates users on the best practices and policies for protecting the organization's data and systems from various threats, such as malware, phishing, social engineering, etc. Security awareness training can reduce the occurrence of malware execution by increasing the users' ability to recognize and avoid malicious links, attachments, downloads, or websites.

Security Awareness seems the most universal option.

Change control makes no sense in the context of the question.

Osman Ceylan — Today at 10:18 AM

education

Question #:37 - (Exam Topic 4)

A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommend?

A. A content filter

B. AWAF

C. A next-generation firewall

D. An IDS

**Answer: C**

**Explanation**

A next-generation firewall (NGFW) is a solution that can defend against malicious actors misusing protocols and being allowed through network defenses. A NGFW is a type of firewall that can perform deep packet inspection, application-level filtering, intrusion prevention, malware detection, and identity-based access control.

A NGFW can also use threat intelligence and behavioral analysis to identify and block malicious traffic based on protocols, signatures, or anomalies. References:

https://www.comptia.org/blog/what-is-a-next-generation-firewall

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:38 - (Exam Topic 4)

Which of the following agreements defines response time, escalation points, and performance metrics?

A. BPA

B. MOU?

C. NDA

D. SLA

**Answer: D**

**Explanation**

A service level agreement (SLA) defines response time, escalation points, and performance metrics. An SLA is a contract between a service provider and a customer that specifies the level and quality of service that will be delivered. An SLA typically includes metrics such as availability, reliability, throughput, latency, security, etc., as well as penalties or remedies for failing to meet them. An SLA also defines how issues will be reported and resolved, how often reviews will be conducted, and how changes will be communicated.

Question #:40 - (Exam Topic 4)

A well-known organization has been experiencing attacks from APTs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the best defense against this scenario?

A. Configuring signature-based antivirus to update every 30 minutes

B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion

C. Implementing application execution in a sandbox for unknown software

D. Fuzzing new files for vulnerabilities if they are not digitally signed

**Answer: C**

**Explanation**

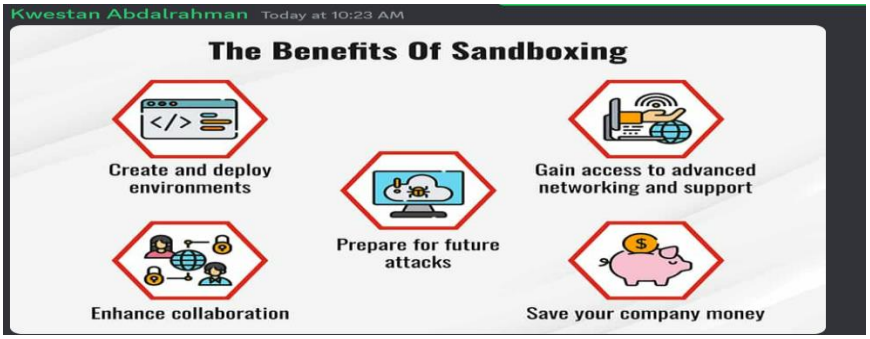
Implementing application execution in a sandbox for unknown software is the best defense against this scenario. A sandbox is a isolated environment that can run applications or code without affecting or being affected by other processes or systems. A sandbox can prevent malicious software from accessing or modifying sensitive data or resources, as well as limit its network communication and system privileges. A sandbox can also monitor and analyze the behavior and output of unknown software to determine if it is benign or malicious.

C: Sandbox environment will ensure malware does not get into the real system.

A: Signature-based antivirus and fuzzing new files for vulnerabilities can be effective against known malware, but they are less effective against new or unknown malware.

B: S/MIME can provide email encryption and authenticity, but it does not provide protection against the installation of custom malware through USB sticks or other channels. Automatic encryption of USB drives upon insertion is also helpful, but it does not prevent the insertion of infected drives in the first place.

D: fuzzing can lead to false positives or false negatives, which can create additional security risks or cause unnecessary disruptions.




Question #:41 - (Exam Topic 4)

The concept of connecting a user account across the systems of multiple enterprises is best known as:

A. federation

B. a remote access policy.

C. multifactor authentication

D. single sign-on.

**Answer: A**

**Explanation**

The concept of connecting a user account across the systems of multiple enterprises is best known as federation. Federation is a process that allows users to authenticate once and access multiple resources or services across different

domains or organizations. For example, a user can use their Google account to sign in to various websites or applications that support federation, without creating separate accounts or passwords for each one. Federation can improve user convenience and security, as well as reduce administrative overhead.

Federated identity allows authorized users to access multiple applications and domains using a single set of credentials. It links a user's identity across multiple identity management systems so they can access different applications securely and efficiently.

Kwestan Abdalrahman — Today at 10:26 AM

Federated identity allows authorized users to access multiple applications and domains using a single set of credentials.

Question #:42 - (Exam Topic 4)

An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the credentials of her popular websites. Which of the following should the company implement?

A. SSO

B. CHAP

C. 802.1X

D. OpenID

**Answer: A**

**Explanation**

SSO stands for Single Sign-On, which is a technology that allows users to log in to multiple websites using a single set of credentials, such as a username and password or a digital certificate. SSO eliminates the need for users to create and remember multiple accounts and passwords for different websites, and simplifies the authentication process. SSO also enhances security by reducing the risk of password reuse, phishing, and identity theft.

An internet company that has created a new collaboration application can implement SSO to allow users to log in to the application with the credentials of other popular websites, such as Google, Facebook, or Twitter. This way, users do not have to create a new account for the application, and can use their existing accounts from other websites that they trust and use frequently. This can increase the user base and the convenience of the application.

Some examples of SSO technologies are OpenID, OAuth, and SAML. These technologies provide different ways of establishing trust and exchanging information between the websites that act as identity providers (IDPs) and the websites that act as relying parties (RPs). The IDPs are the websites that authenticate the users and provide their credentials or attributes to the RPs. The RPs are the websites that accept the users' credentials or attributes from the IDPs and grant them access to their services.

Question #:43 - (Exam Topic 4)

Which of the following security controls is used to isolate a section of the network and its externally available resources from the internal corporate network in order to reduce the number of possible attacks?

A. Faraday cages

B. Air gap

C. Vaulting

D. Proximity readers

**Answer: B**

**Explanation**

An air gap is a security measure that physically isolates a section of the network from any other network or device that could compromise its security. An air gap prevents any unauthorized access, data leakage, or malware infection through network connections, such as Ethernet cables, wireless signals, or Bluetooth devices. An air gap can be used to protect sensitive or critical systems and data from external threats, such as hackers, spies, or cyberattacks.

Faraday cages are physical enclosures that block electromagnetic signals and are typically used to shield electronic equipment from external electromagnetic interference. While they provide physical protection, they are not the same as air gapping in terms of network isolation.

Vaulting typically refers to physical security measures for storing valuable items, but it is not a network security control. Proximity readers are used for access control and authentication but do not provide network isolation.

**Petra Martina Vrancic**

—

**Today at 10:28 AM**

It's like keeping a safe distance to maintain security

Question #:44 - (Exam Topic 4)

A security analyst receives a SIEM alert that someone logged in to the app admin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User [Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account (12345) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (23456) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (23456) result: fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account (45678) result: fail

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.

B. An injection attack is being conducted against a user authentication system.

C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

**Answer: B**

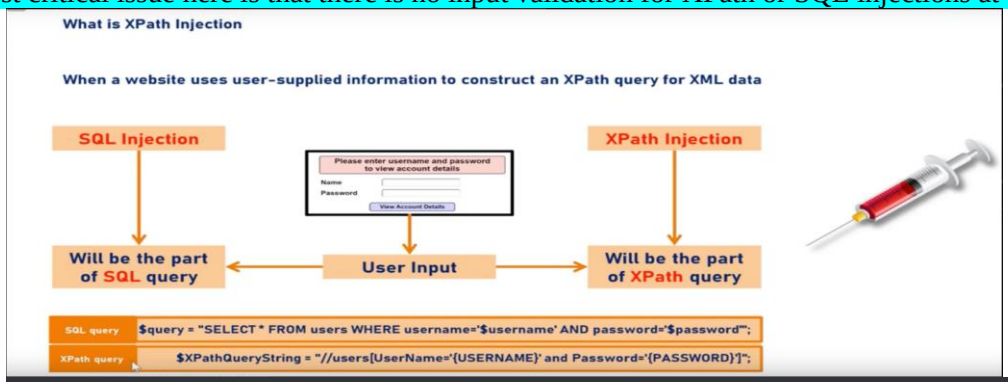
**Explanation**

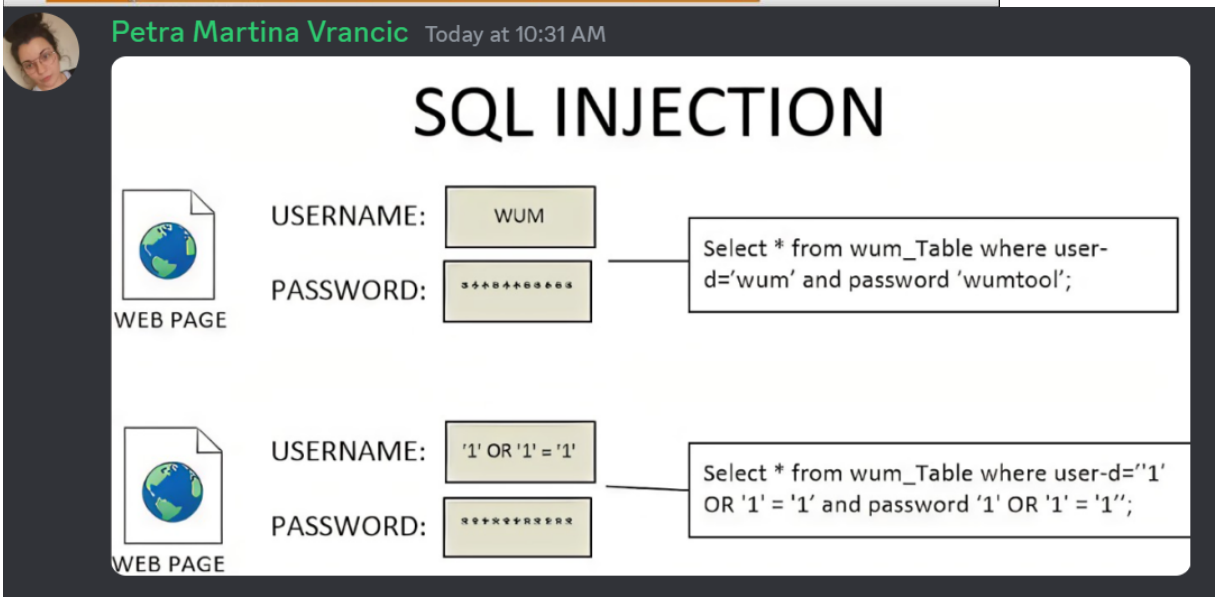
action:open.account: This part of the log entry specifies the action or operation that was attempted. In this case, the action is "open.account," indicating an attempt to open or access an account within the application.

(12345): The number enclosed in parentheses, "12345," may be an identifier associated with the specific account or resource that was targeted or accessed during the "open.account" action. This number could represent an account number, transaction ID, or some other identifier used by the application to reference accounts.

result: fail: This part of the log entry indicates the result or outcome of the "open.account" action. In this case, the result is "fail," suggesting that the attempt to open or access the account was unsuccessful.
So it is not login failures, but the attacker tries to open several accounts which were most probably restricted with access rules or test admin account does not have enough privilege to do that.

The most critical issue here is that there is no input validation for XPath or SQL injections at the application.




Question #:45 - (Exam Topic 4)

Which of the following would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning

B. DNS sinkhole

C. Blocklist

D. Honey pot

**Answer: B**

**Explanation**

A DNS sinkhole would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations. A DNS sinkhole is a technique that involves redirecting malicious or unwanted domain names to an alternative IP address, such as a black hole, a honeypot, or a warning page. A DNS sinkhole can help to prevent or disrupt the communication between infected systems and command-and-control servers, malware distribution sites, phishing sites, or botnets. A DNS sinkhole can also help to identify and isolate infected systems by monitoring the traffic to the sinkhole IP address. References: https://www.comptia.org/blog/what-is-a-dns-sinkhole

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:46 - (Exam Topic 4)

A threat actor used a sophisticated attack to breach a well-known ride-sharing company. The actor posted on social media that this action was in response to the company's treatment of its drivers. Which of the following best describes the type of threat actor?

A. Nation-state

B. Hacktivist

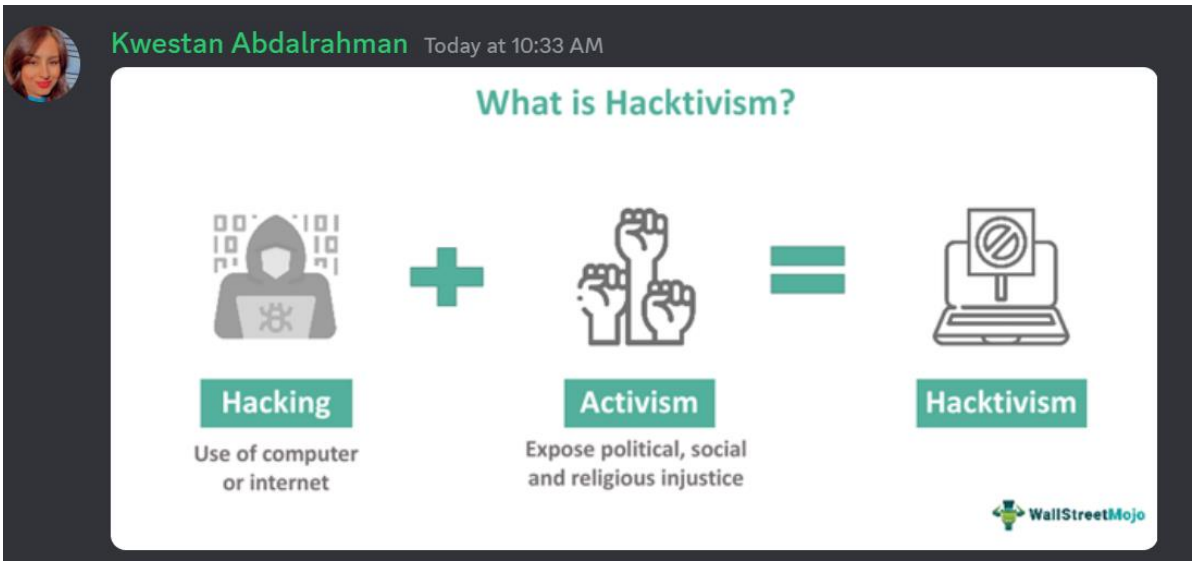
C. Organized crime

D. Shadow IT

**Answer: B**

**Explanation**

A threat actor who used a sophisticated attack to breach a well-known ride-sharing company and posted on social media that this action was in response to the company's treatment of its drivers is most likely a hacktivist. A hacktivist is a person who uses hacking skills to promote a social or political cause, such as human rights, environmentalism, or anti-corporatism.




Question #:47 - (Exam Topic 4)

Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP

B. CSR

C. CA

D. CRC

**Answer: A**

**Explanation**

Online Certificate Status Protocol (OCSP) is used to validate a certificate when it is presented to a user. OCSP is a protocol that allows a client or browser to query the status of a certificate from an OCSP responder, which is a server that maintains and provides the revocation status of certificates issued by a certificate authority (CA). OCSP can help to verify the authenticity and validity of a certificate and prevent the use of revoked or expired certificates. References:

https://www.comptia.org/blog/what-is-ocsp

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Petra Martina Vrancic — Today at 10:36 AM

If the internet connection is down, relying on online services like OCSP (Online Certificate Status Protocol) for certificate validation might pose a challenge. In such cases, a common approach is to use Certificate Revocation Lists (CRLs), which are offline lists maintained by Certificate Authorities (CAs) and contain information about revoked certificates.

Question #:48 - (Exam Topic 4)

During a recent penetration test, a tester plugged a laptop into an Ethernet port in an unoccupied conference room and obtained a valid IP address. Which of the following would have best prevented this avenue of attack?

A. Enabling MAC address filtering

B. Moving printers inside a firewall

C. Implementing 802.1X

D. Using network port security

**Answer: C**

**Explanation**

Implementing 802.1X would have best prevented this avenue of attack. 802.1X is a standard that provides port-based network access control (PNAC), which means that it authenticates devices before allowing them to access network resources through a physical or wireless port. 802.1X can prevent unauthorized devices from obtaining valid IP addresses or accessing sensitive data by requiring them to provide credentials, such as a username and password, a certificate, or a token. 802.1X can also dynamically assign VLANs or firewall rules based on the device identity or role.

Question #:49 - (Exam Topic 4)

The IT department's on-site developer has been with the team for many years. Each time an application is released; the security team is able to identify multiple vulnerabilities. Which of the following would best help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.

B. Prevent data exposure queries.

C. Obfuscate the source code

D. Submit the application to QA before releasing it.

**Answer: D**

**Explanation**

Submitting the application to QA before releasing it would best help the team ensure the application is ready to be released to production. QA stands for quality assurance, which is a process of testing and verifying that a software product meets the specified requirements and standards. QA can help identify and fix any bugs, errors, vulnerabilities, or performance issues before the software is deployed to the end users. QA can also ensure that the software meets the security objectives and complies with the best practices and regulations.
any potential bugs or vulnerabilities in an application before it is released to production. QA testing often includes security

testing, which involves evaluating the application for potential security risks and vulnerabilities. By submitting the application to QA before releasing it, the security team can ensure that any identified vulnerabilities have been addressed and the application is ready to be released to production. This can help to minimize the risk of security breaches and improve the overall security of the application.

A. Limit the use of third-party libraries. - Incorrect, This would imply that the developer is constantly installing third-party libraries.
B. Prevent data exposure queries. - Incorrect, this wouldn't solve the issue of a bad developer.
C. Obfuscate the source code. - Incorrect, this would only make reading the code more difficult, not fix a bad developer.

D. Submit the application to QA before releasing it. - Correct, the Quality Assurance team should always review code prior to production deployment

Question #:50 - (Exam Topic 4)

A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would best prevent this type of attack?

A. Network location

B. Impossible travel time

C. Geolocation

D. Geofencing

**Answer: B**

**Explanation**

Impossible travel time is a security metric that detects anomalous login attempts based on the time and distance between two locations. Impossible travel time can help prevent email account compromises by flagging login attempts that occur within a short time span from locations that are far apart, such as France and Brazil. Impossible travel time can indicate that an attacker has stolen or guessed the user's credentials and is trying to access their email account from another location.

Question #:51 - (Exam Topic 4)

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 way to limit this access?

A. Data masking

B. Encryption

C. Geolocation policy

D. Data sovereignty regulation

**Answer: C**

**Explanation**

A geolocation policy is a policy that restricts access to data or resources based on the physical location of the user or

device. A geolocation policy can be implemented using technologies such as IP address filtering, GPS tracking, VPN blocking, etc. A geolocation policy can help the company's legal department to ensure the documents cannot be accessed by individuals in high-risk countries by denying access requests from those countries.

## Question #:52 - (Exam Topic 4)

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO most likely use?

A. An external security assessment

B. A bug bounty program

C. A tabletop exercise

D. A red-team engagement

**Answer: C**

**Explanation**

A tabletop exercise is a type of simulation exercise that involves discussing hypothetical scenarios and testing the incident response plan in a low-stress environment. A tabletop exercise can help the CSO to validate the business's involvement in the incident response plan by involving key stakeholders, such as senior management, business units, legal department, etc., in the discussion and evaluation of the plan.


## Question #:53 - (Exam Topic 4)

Which of the following holds staff accountable while escorting unauthorized personnel?

A. Locks

B. Badges

C. Cameras

D. Visitor logs

**Answer: D**

**Explanation**

Visitor logs are records of who enters and exits a facility, when, and for what purpose. They can help hold staff accountable while escorting unauthorized personnel by providing evidence of their identity, authorization, and activities. Visitor logs can also help with auditing, incident response, and compliance.

Question #:54 - (Exam Topic 4)

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work best to help identify potential vulnerabilities?

A. ping -S comptia.org -p 80

B. nc -1 -v comptia.crg -p 80

C. nmap comptia.org -p 80 -sv

D. nslookup -port 80 comptia.org

**Answer: C**

**Explanation**

nmap is a network scanning tool that can perform various tasks such as port scanning, service detection, version detection, OS detection, vulnerability scanning, etc… nmap comptia.org -p 80 -sv is a command that scans port 80 (the default port for HTTP) on comptia.org domain name and tries to identify the service name and version running on that port. This can help identify potential vulnerabilities in the web server software by comparing the version with known exploits or patches.

Question #:55 - (Exam Topic 4)

A user's login credentials were recently compromised. During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password. However the trusted website does not use a pop-up for entering user credentials. Which of the following attacks occurred?

A. Cross-site scripting

B. SOL injection

C. DNS poisoning

D. Certificate forgery

**Answer: A**

**Explanation**

In an XSS attack, malicious scripts are injected into web applications, and these scripts can execute in the context of the victim's browser. One common type of XSS is known as "phishing with XSS," where an attacker injects code into a web page to create a fake pop-up window that looks like a legitimate login prompt. Users are then tricked into entering their credentials into the fake pop-up, believing it's part of the trusted website.

In this scenario, when the user input credentials into a pop-up window that wasn't part of the trusted website's legitimate design, it indicates a potential XSS attack. The attacker likely injected malicious code into the website to create a deceptive login pop-up and steal the user's credentials.

SQL Injection (SOL injection) typically involves manipulating SQL queries to exploit database vulnerabilities and is not related to pop-up windows.

DNS poisoning involves manipulating DNS records to redirect traffic, but it doesn't typically involve pop-up windows for credential theft.

Certificate forgery involves creating fake SSL certificates but doesn't directly involve creating deceptive pop-up login prompts.

Question #:56 - (Exam Topic 4)

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement

B. Least privilege

C. An acceptable use policy

D. Off boarding

**Answer: D**

**Explanation**

Off boarding is a security practice that involves revoking access rights and privileges from employees who leave an organization or change their roles. Off boarding can help address the issue of successful logon attempts to access the departed executive’s accounts by disabling or deleting their accounts, changing passwords, collecting devices, etc., as soon as they leave the organization.

Question #:57 - (Exam Topic 4)

Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE

B. CVSS

C. CIA

D. CERT

**Answer: B**

**Explanation**

CVSS stands for Common Vulnerability Scoring System. It is a framework that provides a standardized way to measure the criticality of a vulnerability based on various factors, such as the impact, exploitability, and remediation level of the vulnerability. CVSS assigns a numerical score from 0 to 10 to each vulnerability, where 0 means no risk and 10 means the highest risk. CVSS also provides a qualitative rating for each score, such as low, medium, high, or critical. CVSS helps organizations prioritize the remediation of vulnerabilities based on their severity and potential impact12.

CVE stands for Common Vulnerabilities and Exposures. It is a list of publicly known and standardized identifiers for vulnerabilities and exposures in software and hardware systems. CVE provides a brief description of each vulnerability or exposure, but does not assign a score or rating to them. CVE helps organizations communicate and share information about vulnerabilities and exposures in a consistent and reliable way .

CIA stands for Confidentiality, Integrity, and Availability. It is a model that defines the three main objectives of information security. Confidentiality means protecting data from unauthorized access or disclosure. Integrity means ensuring data is accurate and consistent and has not been tampered with. Availability means ensuring data is accessible and usable by authorized parties when needed. CIA helps organizations design and implement security controls and policies to protect their data and systems .

CERT stands for Computer Emergency Response Team. It is a group of experts who respond to security incidents and provide guidance and assistance to mitigate and prevent cyberattacks. CERT also conducts research and analysis on cybersecurity trends and issues, and disseminates information and best practices to the public. CERT helps organizations improve their security posture and resilience against cyber threats .

For more information on CVSS and other concepts related to vulnerability assessment and management, you can refer to [this video] or [this guide] from CompTIA Security+.

Question #:58 - (Exam Topic 4)

Which of the following is the correct order of volatility from most to least volatile?

A. Memory, temporary filesystems. routing tables, disk, network storage

B. Cache, memory, temporary filesystems, disk, archival media

C. Memory, disk, temporary filesystems. cache, archival media

D. CachSe, disk, temporary filesystems. network storage, archival media

**Answer: B**

**Explanation**

The order of volatility is the order of how quickly data can be lost or changed in a system. The order of volatility is important for digital forensics and evidence collection, as it determines the priority and sequence of data preservation. The correct order of volatility from most to least volatile is cache, memory, temporary filesystems, disk, archival media. Cache is the fastest and most volatile type of memory that stores frequently used data. Memory is the main memory or RAM that stores data for active processes. Temporary filesystems are files that are created and deleted during normal system operations, such as swap files, print spool files, etc. Disk is the permanent storage device that stores data on magnetic or solid-state media. Archival media are devices that store data for long-term preservation, such as optical disks, tapes, etc.

Question #:59 - (Exam Topic 4)

An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian

B. Data controller

C. Data protection officer

D. Data processor

**Answer: B**

**Explanation**

A data controller is an employee role that would determine the purpose of data and how to process it. A data controller is a person or entity that decides why and how personal data is collected, used, stored, shared, or deleted. A data controller has the responsibility to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and to ensure the rights and privacy of data subjects.

The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. So, if your company/organization decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within your organization do so to fulfil your tasks as data controller.

The **data processor** processes personal data only **on behalfof the controller**. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

Data custodian role includes responsibilities for protecting data, including securing, monitoring, and controlling access to it, as well as ensuring data is accurate, complete, and accessible when needed. Ensuring that backups are properly maintained would fall under the responsibilities of a data custodian, as they would be responsible for protecting data and ensuring its availability.

Data custodian: An individual who is responsible for managing the system on which data assets are stored, including being responsible for enforcing access control, encryption, and backup/recovery measures.

✔ Information systems management

Data privacy officer (DPO): Institutional data governance role with responsibility for compliant collection and processing of personal and sensitive data.

✔ Oversight of personally identifiable information (PII) assets

A data controller is a role in data stewardship responsible for determining the purpose for which personal data is collected, used, and processed, and ensuring that this use complies with relevant laws and regulations.
The data controller is also responsible for establishing policies and procedures for managing personal data, including security measures to protect the data from unauthorized access or use. In short, the data controller is responsible for overseeing the collection, storage, and use of personal data to ensure it is handled in an appropriate and ethical manner.

References: https://www.comptia.org/blog/what-is-a-data-controller

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:60 - (Exam Topic 4)

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the most likely cause of the issue?

A. The S/MIME plug-in is not enabled.

B. The SSL certificate has expired.

C. Secure IMAP was not implemented.

D. P0P3S is not supported.

**Answer: A**

**Explanation**

The most likely cause of the issue is that the S/MIME plug-in is not enabled. S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which is a standard that allows email users to encrypt and digitally sign their messages. S/MIME uses public key cryptography and certificates to ensure confidentiality, integrity, authenticity, and non-repudiation of email communications. However, S/MIME requires both the sender and the receiver to have compatible email clients and plug-ins that support S/MIME functionality. If the receiver does not have the S/MIME plug-in enabled, they will not be able to decrypt or verify the encrypted message.

Question #:61 - (Exam Topic 4)

A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity modem response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's BEST course of action?

A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller
B. Ask for the callers name, verify the person's identity in the email directory and provide the requested information over the phone.
C. Write down the phone number of the caller if possible, the name of the person requesting the information, hang up. and notify the organization's cybersecurity officer //////(more official with an action)
D. Request the caller send an email for identity verification and provide the requested information via email to the caller (could send phishing email)

**Answer: C**

In this scenario, the help desk technician should be wary of the person's request as help desk technicians would not have this information. Also, if the person claimed to be from the cybersecurity incident response team, they would more likely to have access to this information anyway, or at least know who to contact.

This is the best course of action for the help desk technician because it can help prevent a potential social engineering attack. Social engineering is a technique that involves manipulating or deceiving people into revealing sensitive information or performing actions that compromise security. The caller may be impersonating a member of the organization’s cybersecurity incident response team to obtain the network’s internal firewall IP address, which could be used for further attacks. The help desk technician should not provide any information over the phone without verifying the caller’s identity and authorization. The help desk technician should also report the incident to the organization’s cybersecurity officer for investigation and response. References: https://www.comptia.org/blog/social-engineering-explained

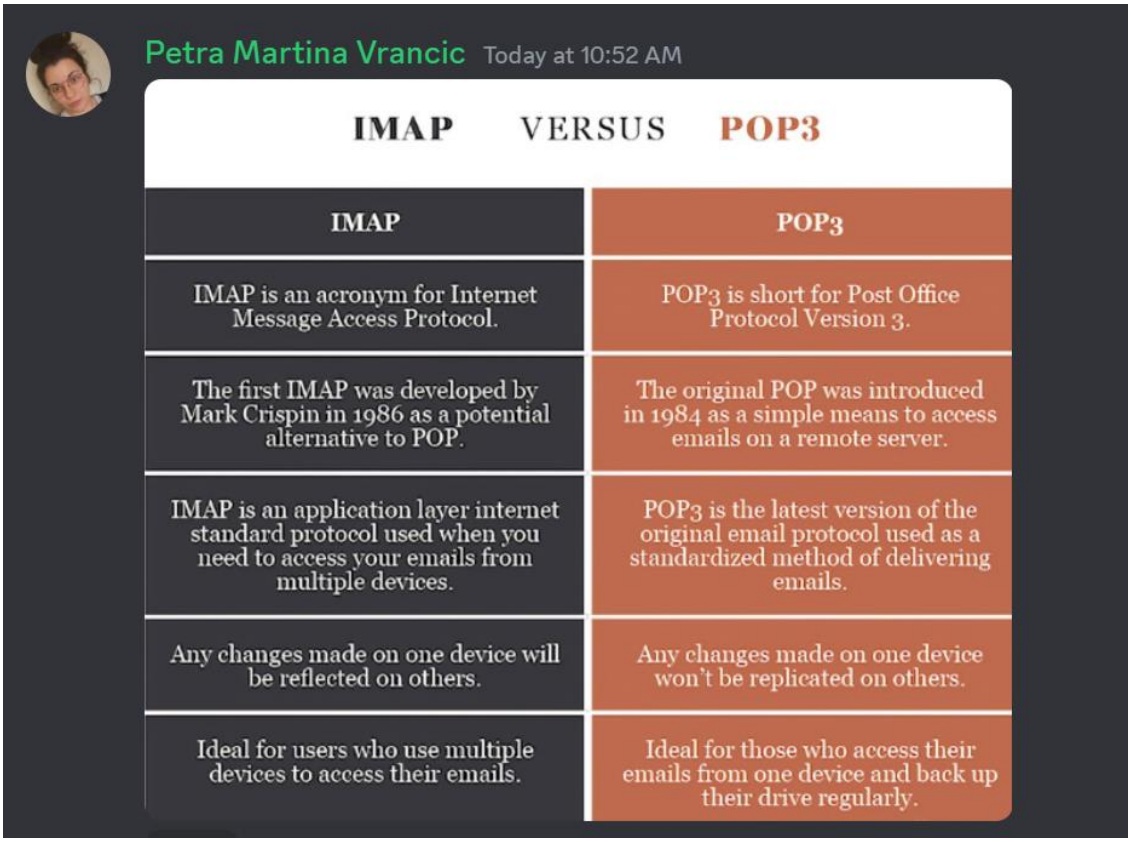
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Petra Martina Vrancic — Today at 10:50 AM

By writing down the caller's information, hanging up, and then notifying the organization's cybersecurity officer, the technician takes a cautious approach to ensure the legitimacy of the request. It allows the organization's security team to investigate the incident and confirm whether the request is valid or potentially malicious.

Kwestan Abdalrahman — Today at 10:50 AM

Post Office Protocol Version 3 (POP3) is an alternative protocol for receiving emails that downloads emails from the server to a local device




Question #:62 - (Exam Topic 4)

An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops

B. Containers

C. Thin clients

D. Workstations

**Answer: C**

**Explanation**

Thin clients are devices that rely on a server or a cloud service to perform most of the processing and storage tasks, while only providing a minimal interface for the user. Thin clients are low-cost solutions that can enable users on the shop floor to log in to the VDI (virtual desktop infrastructure) environment directly, without requiring a full-fledged computer or laptop.


Question #:63 - (Exam Topic 4)

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would most likely have prevented this breach?

A. A firewall

B. A device pin

C. A USB data blocker

D. Biometrics

**Answer: C**

**Explanation**

A USB data blocker is a device that prevents data transfer between a USB device and a host computer, while still allowing charging. This can prevent data breaches caused by malicious USB chargers or devices that may attempt to access or infect the phone's data.

David Berrios — Today at 10:56 AM

A USB data blocker is a device that prevents data exchange when charging a device through a USB port. It blocks the data transfer pins in the USB cable, allowing only power to pass through. Using a USB data blocker would have most likely prevented this data breach scenario where an executive's phone was charged in a public area. By blocking data transfer, sensitive information on the phone cannot be accessed or compromised, even if the phone is connected to a public charging station or an unknown computer.

Question #:64 - (Exam Topic 4)

Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

A. Facial recognition /// you are

B. Six-digit PIN

C. PKI certificate

D. Smart card

**Answer: A**

**Explanation**

Facial recognition is a type of biometric authentication that uses the unique features of a person's face to verify their identity. Facial recognition is not something you know or have, but something you are, which is one of the three factors of authentication. Facial recognition can use various methods and technologies, such as 2D or 3D images, infrared sensors, machine learning and more, to capture, analyze and compare facial data.
Facial recognition can provide a convenient and secure way to authenticate users on personal mobile devices, as it does not require any additional hardware or input from the user. Facial recognition can also be used in conjunction with other factors, such as passwords or tokens, to provide multi-factor authentication. Verified References:

Biometrics - SY0-601 CompTIA Security+ : 2.4 - Professor Messer IT Certification Training Courses https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/biometrics/ (See Facial Recognition)

Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 2: Architecture and Design, Objective 2.4: Given a scenario, implement identity and access management controls.)

Biometric and Facial Recognition - CompTIA Security+ Certification (SY0-501) https://www.oreilly.com/library/view/comptia-security-certification/9781789953091/video9_6.html (See Biometric and Facial Recognition)

Question #:65 - (Exam Topic 4)

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing

B. VM escape

C. Software-defined networking

D. Image forgery

E. Container breakout

**Answer: B**

**Explanation**

The ability of code to target a hypervisor from inside a guest OS is known as VM escape. This is a serious security threat that can compromise the entire virtualized environment and allow an attacker to access other guest OSes or the host OS. VM escape can be achieved by exploiting vulnerabilities in the hypervisor software, the guest OS, or the virtual hardware devices4.

Question #:66 - (Exam Topic 4)

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

GET http://yourbank.com/transfer.do?acctnum=087646959&amount=500000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1

GET http://yourbank.com/transfer.do?acctnum=087646953 &amount=500 HTTP/1.1

Which of the following types of attacks is most likely being conducted?

A. SQLi

B. CSRF

C. Spear phishing

D. API

**Answer: B**

**Explanation**

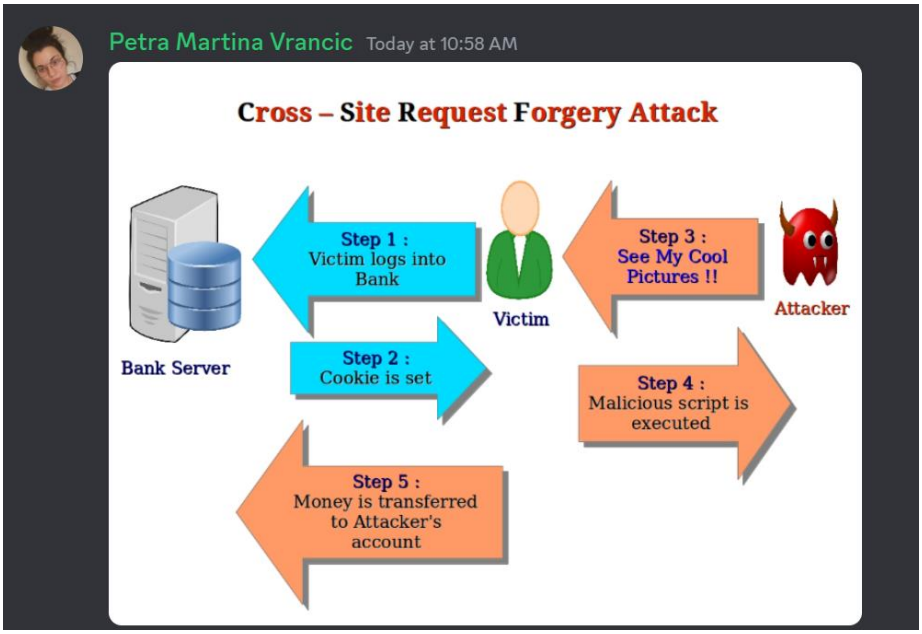
CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated1. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user's session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.

A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution. The output of the web server log does not show any SQL statements or commands.

B. CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.

C. Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email or message that contains a malicious link or attachment3. The output of the web server log does not show any email or message content or headers.

D. API. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API is not an attack method, but rather a way of designing and developing software applications.



Question #:67 - (Exam Topic 4)

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.

B. Data is being exfiltrated.

C. A logic bomb is deleting data.

D. Ransomware is encrypting files.

**Answer: B**

**Explanation**

Data is being exfiltrated when an internal system is sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Data exfiltration is the unauthorized transfer of data from a system or network to an external destination or actor. Data exfiltration can be performed by malicious insiders or external attackers who have compromised the system or network. DNS queries are requests for resolving domain names to IP addresses. DNS queries can be used as a covert channel for data exfiltration by encoding data in the domain names or subdomains and sending them to a malicious DNS server that can decode and collect the data. References:

https://www.comptia.org/blog/what-is-data-exfiltration

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:68 - (Exam Topic 4)

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be best for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall allow list

C. Containment

D. Isolation

**Answer: A**

**Explanation**

Segmentation is a security technique that divides a network into smaller subnetworks or segments based on criteria such as function, role, location, etc. Segmentation can help mitigate the risk of unauthorized access or data leakage by isolating different segments from each other and applying different security policies and controls to each segment. Segmentation can help the security manager to implement a mitigation while maintaining alerting capabilities by separating the smart generator from the internal file server and allowing only necessary communication between them.

Firewall allow list: While firewall rules can control communication, implementing an allow list without proper segmentation might be complex and could inadvertently block legitimate alerting traffic.

Containment: Containment typically refers to isolating a compromised system or malware to prevent further spread. In

this case, containment might be too drastic if the smart generator is not compromised but simply misconfigured.

Isolation: Isolation is similar to containment but may not allow for controlled communication, which may not align with the requirement to maintain alerting capabilities.

Question #:69 - (Exam Topic 4)

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**

Intellectual property is a type of data that is proprietary and unique to an organization. It includes trade secrets and other information that the organization does not want to share with third parties or competitors. Employees in the research and development business unit are most likely to use intellectual property in their day-to-day work activities, as they are involved in creating new products, services, or processes for the organization.
Intellectual property data requires a high level of security and protection, as it can provide a competitive advantage or disadvantage if leaked or stolen.

Encrypted data is not a type of data, but a state of data. Encryption is a method of transforming data into an unreadable format using a key, so that only authorized parties can access it. Encryption can be applied to any type of data, such as intellectual property, critical data, or data in transit.

Critical data is a type of data that is essential for the operation and continuity of an organization. It includes information such as customer records, financial transactions, employee details, and so on. Critical data may or may not be intellectual property, depending on the nature and source of the data. Critical data also requires a high level of security and protection, as it can affect the reputation, performance, or legal compliance of the organization.

Data in transit is not a type of data, but a state of data. Data in transit refers to data that is moving from one location to another over a network, such as the internet, a LAN, or a WAN. Data in transit can be vulnerable to interception, modification, or theft by malicious actors. Data in transit can also be any type of data, such as intellectual property, critical data, or PII.

Question #:70 - (Exam Topic 4)

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker most likely attempting?

A. A spear-phishing attack

B. A watering-hole attack

C. Typosquatting

D. A phishing attack

**Answer: B**

**Explanation**

The attacker is most likely attempting a watering-hole attack. A watering-hole attack is a type of attack that targets a specific group of users by compromising a website that they frequently visit. The attacker then installs malware on the website that infects the visitors' devices or redirects them to malicious sites. The attacker hopes to gain access to the users' credentials, data, or networks by exploiting their trust in the legitimate website.

Question #:71 - (Exam Topic 4)

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would best maintain high-quality video conferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity to have VPN terminators closer to end users

B. Utilizing split tunneling so only traffic for corporate resources is encrypted

C. Purchasing higher bandwidth connections to meet the increased demand

D. Configuring QoS properly on the VPN accelerators

**Answer: D**

**Explanation**

VPN Accelerator splits the path between the VPN server and the destination into shorter paths. That gives a higher combined performance over the entire path. It also uses an advanced network TCP flow control algorithm called BBR to reduce latency and bypass congestion on the internet.
VPN Accelerator uses a combination of advanced VPN technologies to improve connection stability and, in some cases, increase your connection speed by over 400%.

Configuring QoS properly on the VPN accelerators is the best option to maintain high-quality video conferencing while minimizing latency when connected to the VPN. Quality of Service (QoS) helps to prioritize network traffic and ensure that bandwidth-intensive applications like video conferencing receive the necessary bandwidth to function smoothly.

By configuring QoS properly on the VPN accelerators, the video conferencing traffic can be given priority over other less important network traffic, reducing the latency and improving the overall quality of the video conferencing experience.

A: using geographic diversity to have VPN terminators closer to end-users, may help reduce latency by reducing the distance the data needs to travel, but it may not be the most efficient solution as it requires deploying multiple VPN terminators, which can be costly.
B: utilizing split tunneling so only traffic for corporate resources is encrypted, may reduce the load on the VPN, but it can compromise security by exposing remote workers' internet traffic outside the corporate network.

The split tunnel VPN works by dividing your internet connection between two connections. The public network/open server and the private network. By doing so, split-tunnel enables you to leverage VPN to encrypt confidential data while still having direct access to the internet.

C: purchasing higher-bandwidth connections to meet the increased demand, may improve overall network performance but may not address the issue of latency. Additionally, it can be expensive to upgrade bandwidth across the entire network.

Quality of service (QoS)- refers to any technology that manages data traffic to reduce packet loss, latency, and jitter on a network

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_classn/configuration/15-mt/qos-classn-15-mt-book/qos-classn-vpn.pdf

https://www.draytek.com/support/knowledge-base/5175

ensuring a better user experience by minimizing latency and maintaining high-quality connections. This is particularly important when dealing with real-time applications like videoconferencing, where low latency is crucial for a smooth experience.

Question #:72 - (Exam Topic 4)

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red

B. Blue

C. Purple

D. Yellow

**Answer: C**

**Explanation**

A purple team combines both offensive and defensive testing techniques to protect an organization's critical systems. A purple team is a type of cybersecurity team that consists of members from both the red team and the blue team. The red team performs simulated attacks on the organization's systems, while the blue team defends against them. The purple team facilitates the collaboration and communication between the red team and the blue team, and provides feedback and recommendations for improvement. A purple team can help the organization identify and remediate vulnerabilities, enhance security controls, and increase resilience.

References: https://www.comptia.org/blog/red-team-blue-team-purple-team

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:73 - (Exam Topic 4)

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking

D. Side loading

**Answer: C**

**Explanation**

Jailbreaking is the vulnerability that the organization is addressing by adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Jailbreaking is the process of removing the restrictions or limitations imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking can allow users to install unauthorized applications, customize settings, or access system files. However, jailbreaking can also expose the device to security risks, such as malware, data loss, or warranty voidance. References:

https://www.comptia.org/blog/what-is-jailbreaking https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:74 - (Exam Topic 4)

Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would best meet this need?

A. Community

B. Private

C. Public

D. Hybrid

**Answer: A**

**Explanation**

A community cloud deployment strategy would best meet the need of several universities participating in a collaborative research project and needing to share compute and storage resources. A community cloud is a type of cloud service model that provides a shared platform for multiple organizations with common interests, goals, or requirements. A community cloud can offer benefits such as cost savings, scalability, security, privacy, compliance, and collaboration.
References:
https://www.comptia.org/blog/cloud-service-models-saas-paas-and-iaas-explained https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:75 - (Exam Topic 4)

A security administration is trying to determine whether a server is vulnerable to a range of attacks After using a tool, the administrator obtains the following output.

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

A. Memory leak

B. Race condition

C. SQL injection

D. Directory traversal

**Answer: D**

**Explanation**

The directory traversal attack was successfully implemented based on the output. The output shows that the administrator used a tool called Nikto, which is a web server scanner that can detect vulnerabilities and misconfigurations3. The output also shows that Nikto found several files and directories that should not be accessible by web users, such as “/etc/passwd”, “/var/log”, “/etc/shadow”, etc. This indicates that the web server or application has a vulnerability that allows an attacker to manipulate the file path and access arbitrary files on the server. This is a type of attack known as directory traversal, which can lead to information disclosure, privilege escalation, or remote code execution.