Exam Questions SY0-701

CompTIA Security+ Exam

https://www.2passeasy.com/dumps/SY0-701/

NEW QUESTION 1
- (Exam Topic 1)
A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

Answer: DE

Explanation:
MDM solutions emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device. Containerization and application whitelisting are two features of MDM that can help retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.
Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.
Application whitelisting is a technique that allows only authorized applications to run on the device. This way, IT admins can prevent users from installing or using malicious or unapproved applications that might compromise the security of corporate data. Application whitelisting also allows IT admins to control which applications can access corporate resources, such as email servers or cloud storage.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.office1.com/blog/byod-vs-mdm

NEW QUESTION 2
- (Exam Topic 1)
Which of the following is a cryptographic concept that operates on a fixed length of bits?

A. Block cipher
B. Hashing
C. Key stretching
D. Salting

Answer: A

Explanation:
Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

NEW QUESTION 3
- (Exam Topic 1)
A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?

A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
B. Change the password for the guest wireless network every month.
C. Decrease the power levels of the access points for the guest wireless network.
D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

Answer: A

Explanation:
Configuring the guest wireless network on a separate VLAN from the company's internal wireless network will prevent visitors from accessing company resources.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4

NEW QUESTION 4
- (Exam Topic 1)
An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

A. PEAP
B. EAP-FAST
C. EAP-TLS
D. EAP-TTLS

Answer: B

Explanation:
EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 5
- (Exam Topic 1)
If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?

A. Perfect forward secrecy
B. Elliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption

Answer: A

Explanation:
Perfect forward secrecy would ensure that it cannot be used to decrypt all historical data. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

NEW QUESTION 6
- (Exam Topic 1)
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A spill-tunnel VPN
D. Load-balanced servers

Answer: B

Explanation:
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.
To protect the company’s website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

NEW QUESTION 7
- (Exam Topic 1)
A store receives reports that shoppers’ credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers’ credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

A. Identity theft
B. RFID cloning
C. Shoulder surfing
D. Card skimming

Answer: D

Explanation:
The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 5

NEW QUESTION 8
- (Exam Topic 1)
Which of the following would produce the closet experience of responding to an actual incident response scenario?

A. Lessons learned
B. Simulation
C. Walk-through
D. Tabletop

Answer: B

Explanation:
A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident. References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

NEW QUESTION 9
- (Exam Topic 1)
A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.
B. Establish a continuous ping.
C. Utilize an agentless monitor
D. Enable SNMPv3 With passwords.

Answer: C

Explanation:

An agentless monitor is the best method to monitor network operations because it does not require any software or agents to be installed on the devices being monitored, making it less intrusive and less likely to disrupt network operations. This method can monitor various aspects of network operations, such as traffic, performance, and security.
CompTIA Security+ Study Guide, Sixth Edition (SY0-601), Chapter 4: Attacks, Threats, and Vulnerabilities, Monitoring and Detection Techniques, pg. 167-170.

NEW QUESTION 10
- (Exam Topic 1)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO
B. MFA
C. PKI
D. OLP

Answer: A

Explanation:
Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. References:
- CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.
- CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION 10
- (Exam Topic 1)
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. laC
B. MSSP
C. Containers
D. SaaS

Answer: A

Explanation:
laaS (Infrastructure as a Service) allows the creation of virtual networks, automation, and scripting to reduce the area utilized in a datacenter. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4

NEW QUESTION 15
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: B

Explanation:
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.
An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION 16
- (Exam Topic 1)
A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. inability to authenticate
B. Implied trust
C. Lack of computing power
D. Unavailable patch

Answer: D

Explanation:
If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:
- CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

NEW QUESTION 21

- (Exam Topic 1)
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

A. A biometric scanner
B. A smart card reader
C. APKItoken
D. A PIN pad

Answer: A

Explanation:
A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

NEW QUESTION 25
- (Exam Topic 1)
A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server

Answer: B

Explanation:
The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true. References: CompTIA Security+ SY0-601 Exam Objectives: 3.1 Given a scenario, use appropriate software tools to assess the security posture of an organization.

NEW QUESTION 26
- (Exam Topic 1)
The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

Answer: C

Explanation:
To prevent such a breach in the future, the BEST control to use would be Password complexity.
Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.
The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough. References:
- CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 30
- (Exam Topic 1)
A security administrator has discovered that workstations on the LAN are becoming infected with malware.
The cause of the infections appears to be users receiving phishing emails that are bypassing the current
email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

A. Forward proxy
B. HIDS
C. Awareness training
D. A jump server
E. IPS

Answer: C

Explanation:
Awareness training should be implemented to educate users on the risks of clicking on malicious URLs. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

NEW QUESTION 32
- (Exam Topic 1)
Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

A. Penetration testing
B. Code review
C. Wardriving
D. Bug bounty

Answer: D

Explanation:
A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook), Google, Microsoft, and others to improve the security of their products and services
Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

NEW QUESTION 35
- (Exam Topic 1)
An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

A. Apply a DLP solution.
B. Implement network segmentation
C. Utilize email content filtering,
D. isolate the infected attachment.

Answer: B

Explanation:
Network segmentation is the BEST course of action for the analyst to take to prevent further spread of the worm. Network segmentation helps to divide a network into smaller segments, isolating the infected attachment from the rest of the network. This helps to prevent the worm from spreading to other devices within the network. Implementing email content filtering or DLP solution might help in preventing the email from reaching the target or identifying the worm, respectively, but will not stop the spread of the worm. References: CompTIA Security+ Study Guide, Chapter 5: Securing Network Infrastructure, 5.2 Implement Network Segmentation, pp. 286-289

NEW QUESTION 40
- (Exam Topic 1)
Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing

Answer: B

Explanation:
Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life1. Shredding reduces electronic devices to pieces no larger than 2 millimeters2. Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

NEW QUESTION 45
- (Exam Topic 1)
A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.
B. Define the PC firewall rules to limit access.
C. Encrypt the disk on the storage device.
D. Plug the storage device in to the UPS

Answer: A

Explanation:
The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

NEW QUESTION 47
- (Exam Topic 1)

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

A. EDR
B. Firewall
C. HIPS
D. DLP

Answer: D

Explanation:
DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp

NEW QUESTION 51
- (Exam Topic 1)
A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing
B. Phishing
C. Spear phishing
D. Whaling

Answer: A

Explanation:
Vishing is a social engineering attack that uses phone calls or voicemail messages to trick people into divulging sensitive information, such as financial information or login credentials.

NEW QUESTION 52
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

A. Geofencing
B. Self-sovereign identification
C. PKI certificates
D. SSO

Answer: A

Explanation:
Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

NEW QUESTION 57
- (Exam Topic 1)
Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

A. Development
B. Staging
C. Production
D. Test

Answer: B

Explanation:
Staging is an environment in the software development lifecycle that is used to test a modified version of the actual data, current version configurations, and code. This environment compares user-story responses and workflow before the software is released to the production environment. References: CompTIA Security+ Study Guide, Sixth Edition, Sybex, pg. 496

NEW QUESTION 59
- (Exam Topic 1)
A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?

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

Answer: B

Explanation:
Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems. References: CompTIA Security+ Study Guide 601, Chapter 4

NEW QUESTION 64
- (Exam Topic 1)
Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

A. Intelligence fusion
B. Review reports
C. Log reviews
D. Threat feeds

Answer: A

Explanation:
Intelligence fusion is a process that involves aggregating and analyzing data from multiple sources, including artificial intelligence, to provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Glossary, p. 767.

NEW QUESTION 67
- (Exam Topic 1)
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A split-tunnel VPN
D. Load-balanced servers

Answer: B

Explanation:
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.
To protect the company’s website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

NEW QUESTION 69
- (Exam Topic 1)
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alert

Answer: A

Explanation:
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 72
- (Exam Topic 1)
Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

A. White team
B. Purple team
C. Green team
D. Blue team
E. Red team

Answer: A

Explanation:
During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively. They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures.

NEW QUESTION 73
- (Exam Topic 1)

Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

Explanation:
When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 77
- (Exam Topic 1)
Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

Answer: A

Explanation:
A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

NEW QUESTION 79
- (Exam Topic 1)
Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring
B. Honeynets
C. Tcpreplay
D. Data loss prevention

Answer: D

Explanation:
Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

NEW QUESTION 81
- (Exam Topic 1)
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot
B. Differential
C. Full
D. Tape

Answer: B

Explanation:
Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

NEW QUESTION 86
- (Exam Topic 1)
Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps
B. Security guards
C. Video surveillance
D. Fences
E. Bollards
F. Antivirus

Answer: AB

Explanation:
A - a mantrap can trap those personnal with bad intension(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnal from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnal

from entering(preventive+deterrent), and notice those personnal as well(detective)

NEW QUESTION 88
- (Exam Topic 1)
A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:
* Ensure mobile devices can be tracked and wiped.
* Confirm mobile devices are encrypted.
Which of the following should the analyst enable on all the devices to meet these requirements?

A. A Geofencing
B. Biometric authentication
C. Geolocation
D. Geotagging

Answer: A

Explanation:
Geofencing is a technology used in mobile device management (MDM) to allow administrators to define geographical boundaries within which mobile devices can operate. This can be used to enforce location-based policies, such as ensuring that devices can be tracked and wiped if lost or stolen. Additionally, encryption can be enforced on the devices to ensure the protection of sensitive data in the event of theft or loss. References:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7

NEW QUESTION 93
- (Exam Topic 1)
An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?

A. TPM
B. CA
C. SAML
D. CRL

Answer: A

Explanation:
The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

NEW QUESTION 95
- (Exam Topic 1)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.config instead of using the sshd.conf
D. Network services are no longer running on the NAS

Answer: B

Explanation:
SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device12. SSH can encrypt both the authentication information and the data being exchanged between the client and the server2. SSH can be used to access and manage a NAS device remotely3.

NEW QUESTION 96
- (Exam Topic 1)
Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed,
agreed-upon duration of time?

A. PoC
B. Production
C. Test
D. Development

Answer: A

Explanation:
A proof of concept (PoC) environment can be stood up quickly and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time. This environment can utilize either dummy data or actual data. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 97
- (Exam Topic 1)
A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates.
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software

Answer: C

Explanation:
The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run.
References: https://www.techopedia.com/definition/31541/application-whitelisting

NEW QUESTION 99
- (Exam Topic 1)
Which of the following biometric authentication methods is the MOST accurate?

A. Gait
B. Retina
C. Signature
D. Voice

Answer: B

Explanation:
Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

NEW QUESTION 104
- (Exam Topic 1)
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT
B. Ransomware
C. Polymophic
D. A worm

Answer: A

Explanation:
Based on the given information, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan). RATs are often used for stealthy unauthorized access to a victim's computer, and they can evade traditional antivirus software through various sophisticated techniques. In particular, the fact that the malware is communicating with external IP addresses during specific hours suggests that it may be under the control of an attacker who is issuing commands from a remote location. Ransomware, polymorphic malware, and worms are also possible culprits, but the context of the question suggests that a RAT is the most likely answer.

NEW QUESTION 108
- (Exam Topic 1)
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

Answer: A

Explanation:
The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.

NEW QUESTION 113
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery

organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-phishing

NEW QUESTION 118
- (Exam Topic 1)
A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

A. openssl
B. hping
C. netcat
D. tcpdump

Answer: A

Explanation:
To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and
decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic. References:
- CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 123
- (Exam Topic 1)
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask  ..... 255.255.255.0
Default Gateway ..... 10.0.0.1


Internet Address      Physical Address
10.10.255.255         ff-ff-ff-ff-ff-ff
10.0.0.1              aa-aa-aa-aa-aa-aa
10.0.0.256            aa-aa-aa-aa-aa-aa
224.0.0.2             01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding

Answer: B

Explanation:
ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 6, page 271.

NEW QUESTION 125
- (Exam Topic 1)
A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist...
User account 'VMAdmin' does not exist...
User account 'tomcat' wrong password...
User account 'Admin' does not exist...
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing
B. Proper error handling
C. Forward web server logs to a SIEM
D. Input sanitization

Answer: D

Explanation:
Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks. References:
- CompTIA Security+ Certification Exam Objectives 2.2: Given a scenario, implement secure coding techniques.
- CompTIA Security+ Study Guide, Sixth Edition, pages 72-73

NEW QUESTION 128
- (Exam Topic 1)
A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain
B. Domain hijacking
C. DNS poisoning
D. URL redirection

Answer: C

Explanation:
The log entry shows the IP address for "www.example.com" being changed to a different IP address, which is likely the result of DNS poisoning. DNS poisoning occurs when an attacker is able to change the IP address associated with a domain name in a DNS server's cache, causing clients to connect to the attacker's server instead of the legitimate server. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 129
- (Exam Topic 1)
A security analyst reviews a company’s authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

A. Dictionary
B. Rainbow table
C. Spraying
D. Brute-force

Answer: C

Explanation:
Detailed
Password spraying is an attack where an attacker tries a small number of commonly used passwords against a large number of usernames. The goal of password spraying is to avoid detection by avoiding too many failed login attempts for any one user account. The fact that different usernames are being attacked from the same IP address is a strong indication that a password spraying attack is underway.

NEW QUESTION 132
- (Exam Topic 1)
Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

A. Block cipher
B. Hashing
C. Private key
D. Perfect forward secrecy
E. Salting
F. Symmetric keys

Answer: BC

Explanation:
Non-repudiation is the ability to ensure that a party cannot deny a previous action or event. Cryptographic concepts that can be used to implement non-repudiation include hashing and digital signatures, which use a private key to sign a message and ensure that the signature is unique to the signer. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 133
- (Exam Topic 1)
A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

```
http://comptia.org/../../../etc/passwd
```

Which ol the following types of attacks is being attempted and how can it be mitigated?

A. XS
B. mplement a SIEM
C. CSR
D. implement an IPS
E. Directory traversal implement a WAF
F. SQL infection, mplement an IDS

Answer: C

Explanation:
Detailed
The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root

directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4: Securing Application Development and Deployment, p. 191

NEW QUESTION 135
- (Exam Topic 1)
A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

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

Answer: D

Explanation:
A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to them. Therefore, a SIEM represents a detective control.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 138
- (Exam Topic 1)
Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

A. Barricades
B. Thermal sensors
C. Drones
D. Signage
E. Motion sensors
F. Guards
G. Bollards

Answer: AD

Explanation:
Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area.
References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 7

NEW QUESTION 143
- (Exam Topic 1)
A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

A. TOP
B. IMAP
C. HTTPS
D. S/MIME

Answer: D

Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that enables secure email messages to be sent and received. It provides email encryption, as well as digital signatures, which can be used to verify the authenticity of the sender. S/MIME can be used with a variety of email protocols, including POP and IMAP.
References:
- https://www.comptia.org/content/guides/what-is-smime
- CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 139

NEW QUESTION 144
- (Exam Topic 1)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering
B. Zero trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards

Answer: CE

Explanation:
Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources.
Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a

facility and plugging in a remotely accessible device.

NEW QUESTION 147
- (Exam Topic 1)
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps
B. A Telnet session
C. An SSH connection
D. SFTP traffic

Answer: B

Explanation:
The security analyst is likely observing a Telnet session, as Telnet transmits data in plain text format, including usernames and passwords. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware.

NEW QUESTION 149
- (Exam Topic 1)
A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

A. .pfx
B. .csr
C. .pvk
D. .cer

Answer: D

Explanation:
A user should choose the .cer file format to share a public key for secure communication. A .cer file is a public key certificate that can be shared with third parties to enable secure communication.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Cryptography, pp. 301-302.
A public key is a cryptographic key that can be used to encrypt or verify data. A public key file is a file that contains one or more public keys in a specific format. There are different formats for public key files, depending on the application and the algorithm used. Some of the common formats are:
- .pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys.1
- .csr: This is a file format that stores a Certificate Signing Request, which is a message sent to a Certificate Authority (CA) to request a digital certificate. It contains the public key and some information about the identity of the requester. It is also known as PKCS#10 or Certification Request Syntax.2
- .pvk: This is a file format that stores a private key for Microsoft Authenticode code signing. It is used with a .spc file that contains the certificate and public key.3
- .cer: This is a file format that stores a certificate, which is a document that binds a public key to an identity. It is also known as DER or Distinguished Encoding Rules. It is used by some applications such as OpenSSL and Java to read and write certificates.4

NEW QUESTION 153
- (Exam Topic 1)
After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session
Which of the following types of attacks has occurred?

A. Privilege escalation
B. Session replay
C. Application programming interface
D. Directory traversal

Answer: A

Explanation:
"Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user." In this scenario, the red team was able to install malicious software, which would require elevated privileges to access and install. Therefore, the type of attack that occurred is privilege escalation. References: CompTIA Security+ Study Guide, pages 111-112

NEW QUESTION 158
- (Exam Topic 1)
Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking

Answer: C

Explanation:
an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspectio3n45,

which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

NEW QUESTION 163
- (Exam Topic 1)
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD

Answer: CD

Explanation:
In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data. References: CompTIA Security+ Study Guide 601, Chapter 11

NEW QUESTION 168
- (Exam Topic 1)
During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s
B. chflags
C. chmod
D. lsof
E. setuid

Answer: C

Explanation:
The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 172
- (Exam Topic 1)
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.
C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.

Answer: D

Explanation:
An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION 174
- (Exam Topic 1)
Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

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

Answer: C

Explanation:
Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment. References: CompTIA Security+ Certification Exam Objectives 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.

NEW QUESTION 178
- (Exam Topic 1)
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.

C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution

Answer: BC

Explanation:
When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft.
References: CompTIA Security+ Study Guide, pages 217-218, 225-226

NEW QUESTION 181
- (Exam Topic 1)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity

Answer: B

Explanation:
A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 184
- (Exam Topic 1)
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption

Answer: C

Explanation:
One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

NEW QUESTION 187
- (Exam Topic 1)
A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

A. Cellular
B. NFC
C. Wi-Fi
D. Bluetooth

Answer: B

Explanation:
NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

NEW QUESTION 192
- (Exam Topic 1)
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

A. Implement input validations
B. Deploy MFA
C. Utilize a WAF
D. Configure HIPS

Answer: A

Explanation:
Implementing input validations will prevent code injection attacks by verifying the type and format of user input. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION 196
- (Exam Topic 1)
An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP
B. SAML
C. SSO
D. Kerberos

Answer: C

Explanation:
Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials. References: CompTIA Security+ Study Guide 601, Chapter 6

NEW QUESTION 197
- (Exam Topic 1)
A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been Which of the following statements BEST explains the issue?

A. OpenID is mandatory to make the MFA requirements work
B. An incorrect browser has been detected by the SAML application
C. The access device has a trusted certificate installed that is overwriting the session token
D. The user’s IP address is changing between logins, bur the application is not invalidating the token

Answer: D

NEW QUESTION 202
- (Exam Topic 1)
A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

A. 135
B. 139
C. 143
D. 161
E. 443
F. 445

Answer: BF

Explanation:
To protect the servers in the company’s DMZ from external attack due to the new vulnerability in the SMB
protocol on the Windows systems, the security administrator should block TCP ports 139 and 445 for all external inbound connections to the DMZ.
SMB uses TCP port 139 and 445. Blocking these ports will prevent external attackers from exploiting the vulnerability in SMB protocol on Windows systems. Blocking TCP ports 139 and 445 for all external inbound connections to the DMZ can help protect the servers, as these ports are used by SMB protocol. Port 135 is also associated with SMB, but it is not commonly used. Ports 143 and 161 are associated with other protocols and services. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.4 Compare and contrast network architecture and technologies.

NEW QUESTION 205
- (Exam Topic 1)
A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man in the browser
E. Bluejacking

Answer: A

Explanation:
The most likely cause of the enterprise data being compromised from a local database is Shadow IT. Shadow IT is the use of unauthorized applications or devices by employees to access company resources. In this case, the sales director's laptop was stolen, and the attacker was able to use it to access the local database, which was not secured properly, allowing unauthorized access to sensitive data. References:
- CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 207
- (Exam Topic 1)
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

A. whaling.
B. smishing.
C. spear phishing
D. vishing

Answer: C

Explanation:
The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

NEW QUESTION 210
- (Exam Topic 1)
A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares Which of the following should the company implement?

A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI

Answer: A

Explanation:
Detailed
Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p. 465

NEW QUESTION 213
- (Exam Topic 1)
Which of the following involves the inclusion of code in the main codebase as soon as it is written?

A. Continuous monitoring
B. Continuous deployment
C. Continuous Validation
D. Continuous integration

Answer: D

Explanation:
Detailed
Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs.

NEW QUESTION 216
- (Exam Topic 1)
A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

A. DoS attack
B. ARP poisoning
C. DNS spoofing
D. NXDOMAIN attack

Answer: C

Explanation:
The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

NEW QUESTION 217
- (Exam Topic 1)
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ
B. A VPN a
C. A VLAN
D. An ACL

Answer: D

Explanation:
After segmenting the network, a network manager can use an access control list (ACL) to control the traffic between the segments. An ACL is a set of rules that

permit or deny traffic based on its characteristics, such as the source and destination IP addresses, protocol type, and port number. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 219
- (Exam Topic 1)
Which of the following conditions impacts data sovereignty?

A. Rights management
B. Criminal investigations
C. Healthcare data
D. International operations

Answer: D

Explanation:
Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. References:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 221
- (Exam Topic 1)
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host

Answer: B

Explanation:
To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

NEW QUESTION 222
- (Exam Topic 1)
Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

A. Phishing
B. Vishing
C. Smishing
D. Spam

Answer: C

Explanation:
Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:
Learn login credentials to accounts via credential phishing Discover private data like social security numbers
Send money to the attacker Install malware on a phone
Establish trust before using other forms of contact like phone calls or emails
Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.
Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

NEW QUESTION 225
- (Exam Topic 1)
A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
        Server: rogue.comptia.com
        Address: 172.16.1.250
        Non-authoritative answer:
        Name: software-solution.com
        Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC

```
helpdesk> nslookup software-solution.com
        Server: dns.comptia.com
        Address: 172.16.1.1
        Non-authoritative answer:
        Name: software-solution.com
        Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

A. Domain hijacking

B. DNS poisoning
C. MAC flooding
D. Evil twin

Answer: B

Explanation:
DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, such as an IP address. This results in traffic being diverted to the attacker's computer (or any other malicious destination).
DNS poisoning can be performed by various methods, such as:
- Intercepting and forging DNS responses from legitimate servers
- Compromising DNS servers and altering their records
- Exploiting vulnerabilities in DNS protocols or implementations
- Sending malicious emails or links that trigger DNS queries with poisoned responses According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential
indicators to determine the type of attack:
"DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record."
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

NEW QUESTION 229
- (Exam Topic 1)
A company is concerned about individuals dnvmg a car into the building to gam access Which of the following security controls would work BEST to prevent this from happening?

A. Bollard
B. Camera
C. Alarms
D. Signage
E. Access control vestibule

Answer: A

Explanation:
A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short,
vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

NEW QUESTION 234
- (Exam Topic 1)
The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol
B. Encryption type
C. WAP placement
D. VPN configuration

Answer: C

Explanation:
WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.
WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:
- Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
- Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
- Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION 239
- (Exam Topic 1)
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates

Answer: C

Explanation:
When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network. This prevents the malware from spreading and potentially infecting other hosts. Adding a

deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. References: CompTIA Security+ Study Guide, pages 113-114

NEW QUESTION 241
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0c-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking

Answer: C

Explanation:
The output of the “netstat -ano” command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.
The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client’s browser.
Based on the output of the “netstat -ano” command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.
ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION 246
- (Exam Topic 1)
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

Answer: A

Explanation:
The Service Level Agreement (SLA) is a contract between the cloud service provider and the organization that stipulates the exact requirements for the cloud provider. It outlines the level of service that the provider must deliver, including the minimum uptime percentage, support response times, and the remedies and penalties for failing to meet the agreed-upon service levels.

NEW QUESTION 248
- (Exam Topic 1)
one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key
B. DNS hacking to reroute traffic
C. Brute force to the access point
D. A SSL/TLS downgrade

Answer: D

Explanation:
The scenario describes a Man-in-the-Middle (MitM) attack where the attacker intercepts traffic and downgrades the secure SSL/TLS connection to an insecure HTTP connection. This type of attack is commonly known as SSL/TLS downgrade attack or a stripping attack. The attacker is able to see and modify the communication between the client and server.

NEW QUESTION 250
- (Exam Topic 1)
An analyst Is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:

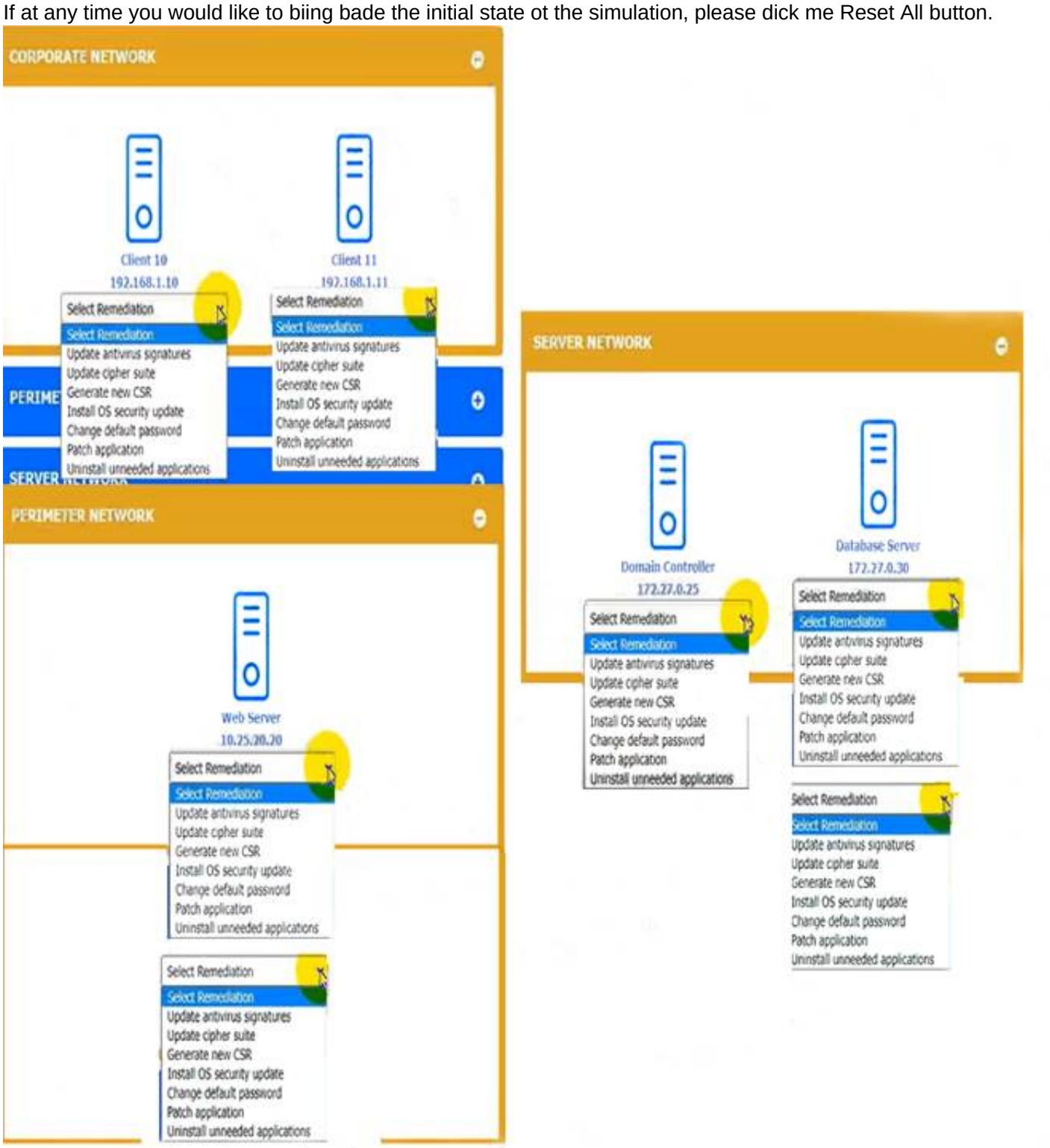
```
PORT     STATE
21/tcp   filtered
22/tcp   open
23/tcp   open
443/tcp  open
```

Which of the following should the analyst recommend to disable?

A. 21/tcp
B. 22/tcp
C. 23/tcp
D. 443/tcp

Answer: A

NEW QUESTION 252
- (Exam Topic 1)
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce. Remediation options may be selected multiple times, and some devices may require more than one
remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.

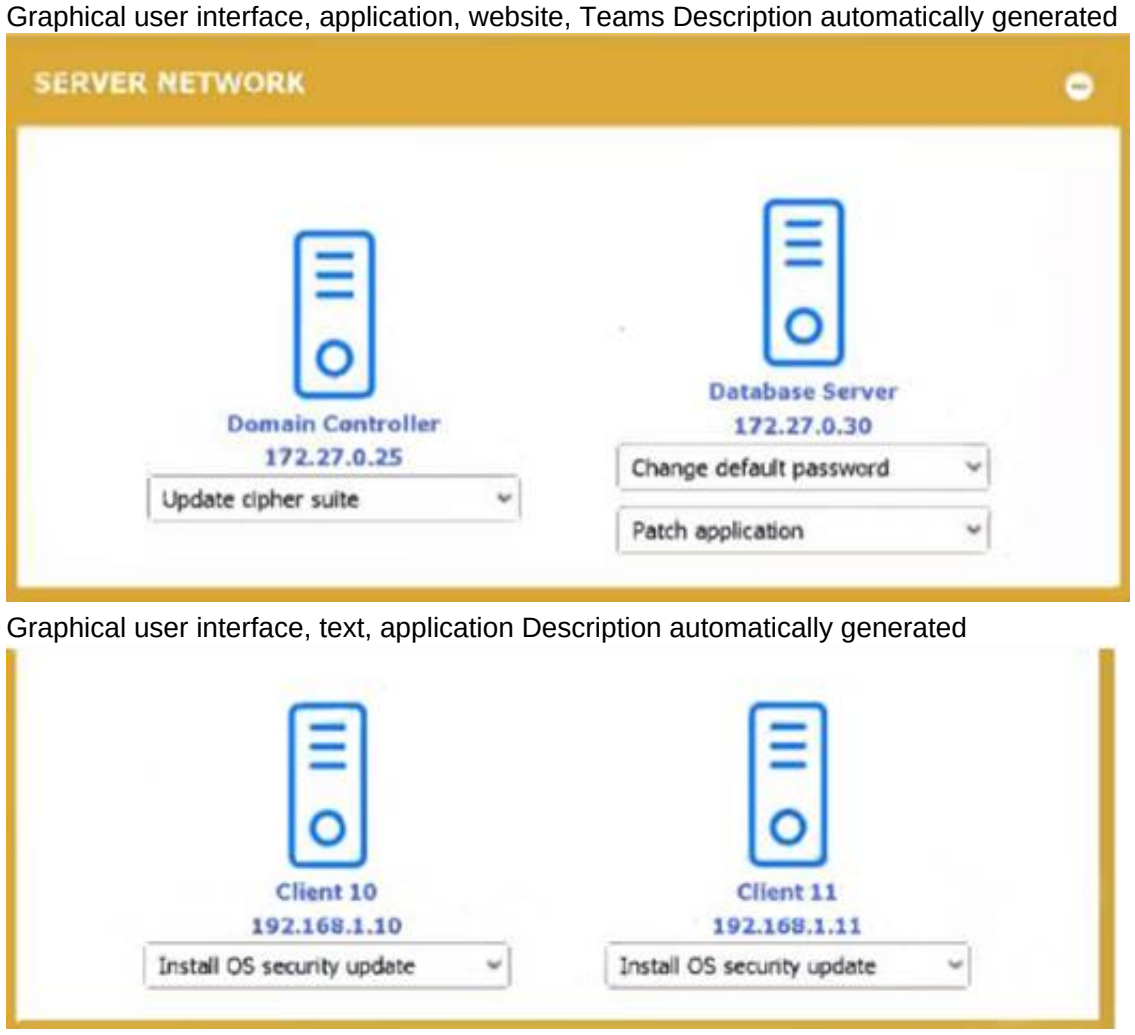


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, website, Teams Description automatically generated



Graphical user interface, text, application Description automatically generated

NEW QUESTION 256
- (Exam Topic 1)
Which of the following controls would provide the BEST protection against tailgating?

A. Access control vestibule
B. Closed-circuit television
C. Proximity card reader
D. Faraday cage

Answer: A

Explanation:
Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area. They are effective at preventing tailgating, as only one person can pass through each door at a time.
References:
- https://www.comptia.org/content/guides/what-is-a-mantrap
- CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 222

NEW QUESTION 258
- (Exam Topic 1)
The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

A. Account audits
B. AUP
C. Password reuse
D. SSO

Answer: A

Explanation:
Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.
To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify

inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

NEW QUESTION 260
- (Exam Topic 1)
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS
B. Implementing a new SSID for every event hosted by the college that has visitors
C. Creating a unique PSK for every visitor when they arrive at the reception area
D. Deploying a captive portal to capture visitors' MAC addresses and names

Answer: D

Explanation:
A captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

NEW QUESTION 264
- (Exam Topic 1)
A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering
B. 802.1X
C. Captive portal
D. WPS

Answer: D

Explanation:
The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4: Identity and Access Management

NEW QUESTION 267
- (Exam Topic 1)
An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware
B. Hash substitution
C. Collision
D. Phishing

Answer: B

Explanation:
This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

NEW QUESTION 271
- (Exam Topic 1)
During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physical move the PC to a separate internet pint of presence
B. Create and apply micro segmentation rules.
C. Emulate the malware in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:
To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary. References:
https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/

NEW QUESTION 274
- (Exam Topic 1)
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production

B. Test
C. Staging
D. Development

Answer: D

Explanation:
A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 275
- (Exam Topic 1)
An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:
•Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
•Internal users in question were changing their passwords frequently during that time period.
•A jump box that several domain administrator users use to connect to remote devices was recently compromised.
•The authentication method used in the environment is NTLM.
Which of the following types of attacks is MOST likely being used to gain unauthorized access?

A. Pass-the-hash
B. Brute-force
C. Directory traversal
D. Replay

Answer: A

Explanation:
The suspicious activity reported by the application owner, combined with the recent compromise of the jump box and the use of NTLM authentication, suggests that an attacker is likely using a pass-the-hash attack to gain unauthorized access to the financial application. This type of attack involves stealing hashed passwords from memory and then using them to authenticate as the compromised user without needing to know the user's plaintext password. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 277
- (Exam Topic 1)
An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box
B. Red-leam
C. Bug bounty
D. Gray-box
E. Black-box

Answer: C

Explanation:
Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION 281
- (Exam Topic 2)
A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

A. Script kiddie
B. Insider threats
C. Malicious actor
D. Authorized hacker

Answer: D

Explanation:
An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

NEW QUESTION 286
- (Exam Topic 2)
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

Answer: D

Explanation:
Organized crime is a term that describes groups of criminals who operate in a coordinated and systematic manner to pursue illicit activities for profit. Organized crime groups often use sophisticated tools and techniques to evade law enforcement and exploit vulnerabilities in various sectors, such as finance, transportation, or healthcare. Organized crime groups may also collaborate with other criminal groups or actors to share resources, information, or expertise.
Ransomware as a service (RaaS) is an example of a business model used by organized crime groups to conduct ransomware and extortion attacks. RaaS is an arrangement between an operator, who develops and maintains the tools to power extortion operations, and an affiliate, who deploys the ransomware payload. When the affiliate conducts a successful ransomware and extortion attack, both parties profit. The RaaS model lowers the barrier to entry for attackers who may not have the skill or technical wherewithal to develop their own tools but can manage ready-made penetration testing and sysadmin tools to perform attacks12.
Insider threat is a term that describes individuals who have legitimate access to an organization's systems or data and use it for malicious purposes, such as theft, sabotage, or espionage. Insider threats may be motivated by various factors, such as greed, revenge, ideology, or coercion. Insider threats may also be unintentional, such as when an employee falls victim to phishing or social engineering.
Hacktivist is a term that describes individuals or groups who use hacking or cyberattacks to promote a political or social cause. Hacktivists may target governments, corporations, or other entities that they perceive as oppressive, corrupt, or unethical. Hacktivists may also use cyberattacks to expose information, disrupt services, or deface websites.
Nation-state is a term that describes a sovereign state that has a centralized government and a defined territory. Nation-state actors are individuals or groups who conduct cyberattacks on behalf of or with the support of a nation-state. Nation-state actors may target other states, organizations, or individuals for various reasons, such as espionage, sabotage, influence, or retaliation.

NEW QUESTION 290
- (Exam Topic 2)
Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

A. Access control
B. Syslog
C. Session Initiation Protocol traffic logs
D. Application logs

Answer: B

Explanation:
Syslogs are log files that are generated by devices on the network and contain information about network
activity, including user logins, device connections, and other events. By analyzing these logs, the IT security team can identify the source of the threatening voicemail messages and take the necessary steps to address the issue

NEW QUESTION 291
- (Exam Topic 2)
A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race Which of the following best describes this type of information?

A. Sensitive
B. Non-Pll
C. Private
D. Confidential

Answer: B

Explanation:
Non-PII stands for non-personally identifiable information, which is any data that does not directly identify a specific individual. Non-PII can include information such as job title, business phone number, location, first
initial with last name, and race. Non-PII can be used for various purposes, such as statistical analysis, marketing, or research. However, non-PII may still pose some privacy risks if it is combined or linked with other data that can reveal an individual's identity.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.investopedia.com/terms/n/non-personally-identifiable-information-npii.asp

NEW QUESTION 293
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

A. A spraying attack was used to determine which credentials to use
B. A packet capture tool was used to steal the password
C. A remote-access Trojan was used to install the malware
D. A directory attack was used to log in as the server administrator

Answer: B

Explanation:
Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References: https://www.comptia.org/content/guides/what-is-network-security

NEW QUESTION 294
- (Exam Topic 2)
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.

B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective

Answer: B

Explanation:
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION 299
- (Exam Topic 2)
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal m a secure manner?

A. Digital signatures
B. Key exchange
C. Salting
D. PPTP

Answer: B

Explanation:
Key exchange Short
Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References: https://www.comptia.org/content/guides/what-is-encryption

NEW QUESTION 301
- (Exam Topic 2)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

A. The vulnerability scanner was not properly configured and generated a high number of false positives
B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Answer: A

Explanation:
The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

NEW QUESTION 304
- (Exam Topic 2)
Which of the following would satisfy three-factor authentication requirements?

A. Password, PIN, and physical token
B. PIN, fingerprint scan, and ins scan
C. Password, fingerprint scan, and physical token
D. PIN, physical token, and ID card

Answer: C

Explanation:
Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as
per the organization's security policies.

NEW QUESTION 305
- (Exam Topic 2)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).

A. MAC filtering
B. Zero trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards.

Answer: AC

Explanation:
MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.
Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

NEW QUESTION 308
- (Exam Topic 2)
Which Of the following is a primary security concern for a setting up a BYOD program?

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

Answer: D

Explanation:
Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device’s operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc

NEW QUESTION 313
- (Exam Topic 2)
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
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)

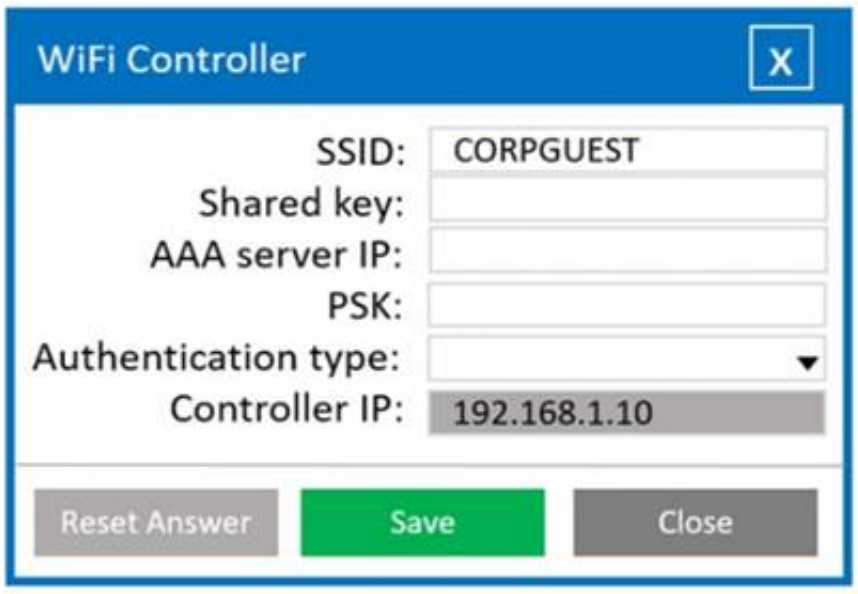
NEW QUESTION 315
- (Exam Topic 2)
A security administrator needs to provide secure access to internal networks for external partners The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

A. Kerberos
B. SSL/TLS
C. IPSec
D. SSH

Answer: C

Explanation:
IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption,
authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References:
https://www.comptia.org/content/guides/what-is-vpn

NEW QUESTION 317
- (Exam Topic 2)
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.
Perform the following steps:
* 1. Configure the RADIUS server.
* 2. Configure the WiFi controller.
* 3. Preconfigure the client for an incoming guest. The guest AD credentials are:
User: guest01 Password: guestpass



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Wifi Controller SSID: CORPGUEST
SHARED KEY: Secret
AAA server IP: 192.168.1.20
PSK: Blank
Authentication type: WPA2-EAP-PEAP-MSCHAPv2 Controller IP: 192.168.1.10
Radius Server Shared Key: Secret
Client IP: 192.168.1.10
Authentication Type: Active Directory Server IP: 192.168.1.20
Wireless Client SSID: CORPGUEST
Username: guest01 Userpassword: guestpass PSK: Blank
Authentication type: WPA2-Enterprise

NEW QUESTION 318
- (Exam Topic 2)
A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

A. pcap reassembly
B. SSD snapshot
C. Image volatile memory
D. Extract from checksums

Answer: C

Explanation:
The best technique for the digital forensics team to use to obtain a sample of the malware binary is to image volatile memory. Volatile memory imaging is a process of collecting a snapshot of the contents of a computer's RAM, which can include active malware programs. According to the CompTIA Security+ SY0-601 Official Text Book, volatile memory imaging can be used to capture active malware programs that are running in memory, but have not yet been committed to disk. This technique is especially useful in cases where the malware is designed to self-destruct or erase itself from the disk after execution.

NEW QUESTION 320
- (Exam Topic 2)
A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?

A. NDA
B. BPA
C. AUP
D. SLA

Answer: C

Explanation:
AUP stands for acceptable use policy, which is a document that defines the rules and guidelines for using an organization’s network, systems, devices, and resources. An AUP typically covers topics such as authorized and unauthorized activities, security requirements, data protection, user responsibilities, and consequences for violations. An AUP can help prevent non-work-related software installation on company-issued devices by clearly stating what types of software are allowed or prohibited, and what actions will be taken if users do not comply with the policy.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

NEW QUESTION 321
- (Exam Topic 2)
A web server has been compromised due to a ransomware attack. Further Investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago
B. The last known-good configuration stored by the operating system
C. The last full backup that was conducted seven days ago
D. The baseline OS configuration

Answer: A

Explanation:
The last incremental backup that was conducted 72 hours ago would be the best option to restore the services to a secure state, as it would contain the most recent data before the ransomware infection. Incremental backups only store the changes made since the last backup, so they are faster and use less storage space than full backups. Restoring from an incremental backup would also minimize the data loss and downtime caused by the ransomware attack. References:
- https://www.comptia.org/blog/mature-cybersecurity-response-to-ransomware
- https://www.youtube.com/watch?v=HszU4nEAlFc

NEW QUESTION 324
- (Exam Topic 2)
A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

A. Directory traversal
B. SQL injection
C. Privilege escalation
D. Cross-site scripting

Answer: B

Explanation:
SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement “SELECT * FROM customername” to retrieve all data from the customername table in the database.

NEW QUESTION 327
- (Exam Topic 2)
An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan
B. The risk management plan
C. The communication plan
D. The incident response plan

Answer: A

Explanation:
A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

NEW QUESTION 332
- (Exam Topic 2)
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?

A. SOC2
B. CSA
C. CSF
D. 1SO 31000

Answer: A

Explanation:
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization’s systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3: https://www.csagroup.org/store/product/50072454os/ 1: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

NEW QUESTION 336
- (Exam Topic 2)
A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

A. Tokenization
B. Input validation

C. Code signing
D. Secure cookies

Answer: B

Explanation:
Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

NEW QUESTION 340
- (Exam Topic 2)
A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

A. Install DLP software to prevent data loss.
B. Use the latest version of software.
C. Install a SIEM device.
D. Implement MDM.
E. Implement a screened subnet for the web server.
F. Install an endpoint security solution.
G. Update the website certificate and revoke the existing ones.
H. Deploy additional network sensors.

Answer: BEF

NEW QUESTION 345
- (Exam Topic 2)
The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

A. Privilege escalation
B. Buffer overflow
C. Resource exhaustion
D. Cross-site scripting

Answer: B

Explanation:
A buffer overflow attack occurs when an attacker inputs more data than the buffer can store, causing the excess data to overwrite adjacent memory locations and corrupt or execute code1. In this case, the attacker entered thousands of characters into a text box that was intended for phone numbers, which are much shorter. This could result in a buffer overflow attack that compromises the web application or server. The other options are not related to this scenario. Privilege escalation is when an attacker gains unauthorized access to higher-level privileges or resources2. Resource exhaustion is when an attacker consumes all the available resources of a system, such as CPU, memory, disk space, etc., to cause a denial of service3. Cross-site scripting is when an attacker injects malicious code into a web page that is executed by the browser of a victim who visits the page.
References: 1: https://www.fortinet.com/resources/cyberglossary/buffer-overflow 2: https://www.imperva.com/learn/application-security/privilege-escalation/ 3: https://www.imperva.com/learn/application-security/resource-exhaustion/ : https://owasp.org/www-community/attacks/xss/

NEW QUESTION 349
- (Exam Topic 2)
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

NEW QUESTION 351
- (Exam Topic 2)
Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing
B. DNS sinkhole
C. TLS inspection

D. Data masking

Answer: C

Explanation:
TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity. References: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

NEW QUESTION 353
- (Exam Topic 2)
A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

A. Coniguring replication of the web servers at the primary site to offline storage
B. Constructing the secondary site in a geographically disperse location
C. Deploying load balancers at the primary site
D. Installing generators
E. Using differential backups at the secondary site
F. Implementing hot and cold aisles at the secondary site

Answer: BD

Explanation:
* B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. References: 1
CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1 : Explain the importance of secure staging deployment concepts 2
CompTIA Security+ Certification Exam
Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application
development, deployment, and automation concepts 3
CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

NEW QUESTION 354
- (Exam Topic 2)
Which Of the following vulnerabilities is exploited an attacker Overwrite a reg-ister with a malicious address that changes the execution path?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

Answer: C

Explanation:
A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can
hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

NEW QUESTION 356
- (Exam Topic 2)
An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

A. Disconnect every host from the network.
B. Run an AV scan on the entire
C. Scan the hosts that show signs of
D. Place all known-infected hosts on an isolated network

Answer: D

Explanation:
Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

NEW QUESTION 361
- (Exam Topic 2)
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: AB

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

NEW QUESTION 366
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-701 Product From:

https://www.2passeasy.com/dumps/SY0-701/

Money Back Guarantee

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

* SY0-701 Practice Questions Verified by Expert Senior Certified Staff

* SY0-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year