Exam Questions SY0-701

CompTIA Security+ Exam

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

NEW QUESTION 1
- (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 2
- (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 3
- (Exam Topic 1)
A retail company that is launching @ new website to showcase the company’s product line and other information for online shoppers registered the following URLs:
* www companysite com
* shop companysite com
* about-us companysite com contact-us. companysite com secure-logon company site com
Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

A. A self-signed certificate
B. A root certificate
C. A code-signing certificate
D. A wildcard certificate
E. An extended validation certificate

Answer: D

Explanation:
The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.
The retail company should use a wildcard certificate if it is concerned with convenience and c1o2s.tA wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (*) in the domain name field, and can secure multiple subdomains of the primary domain1

NEW QUESTION 4
- (Exam Topic 1)
A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backup followed by different backups

Answer: B

Explanation:
The best backup strategy for minimizing the number of backups that need to be restored in case of data loss is full backups followed by incremental backups. This strategy allows for a complete restoration of data by restoring the most recent full backup followed by the most recent incremental backup. Reference: CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) page 126

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system Which of the following would be BEST suited for this task?

A. Social media analysis
B. Annual information security training
C. Gamification
D. Phishing campaign

Answer: D

Explanation:
A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

NEW QUESTION 7
- (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 8
- (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 9
- (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 10
- (Exam Topic 1)
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key

Answer: B

Explanation:
When selecting an encryption method for data that needs to remain confidential for a specific length of time, the longevity of the encryption algorithm should be considered to ensure that the data remains secure for the required period. References: CompTIA Security+ Certification Exam Objectives - 3.2 Given a scenario, use appropriate cryptographic methods. Study Guide: Chapter 4, page 131.

NEW QUESTION 10
- (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 11
- (Exam Topic 1)
Which of the following authentication methods is considered to be the LEAST secure?

A. TOTP
B. SMS
C. HOTP
D. Token key

Answer: B

Explanation:
SMS-based authentication is considered to be the least secure among the given options. This is because SMS messages can be intercepted or redirected by attackers through techniques such as SIM swapping,
man-in-the-middle attacks, or exploiting weaknesses in the SS7 protocol used by mobile networks. Additionally, SMS messages can be compromised if a user's phone is lost, stolen, or infected with malware. In contrast, TOTP (Time-based One-Time Password), HOTP (HMAC-based One-Time Password), and token keys are more secure as they rely on cryptographic algorithms or physical devices to generate one-time use codes, which are less susceptible to interception or unauthorized access. Reference: 1. National Institute of Standards and Technology (NIST). (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

NEW QUESTION 12
- (Exam Topic 1)
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving
B. Shoulder surfing
C. Information elicitation
D. Credential harvesting

Answer: A

Explanation:
Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.
References:
- CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

NEW QUESTION 15

- (Exam Topic 1)
An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM
B. CASB
C. TPM
D. DLP

Answer: A

Explanation:
Hardware Security Module (HSM) is a network appliance designed to securely store cryptographic keys and perform cryptographic operations. HSMs provide a secure environment for key management and can be used to keep cryptographic keys safe from theft, loss, or unauthorized access. Therefore, an enterprise can achieve the goal of keeping cryptographic keys in a safe manner by using an HSM appliance. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 2.0: Technologies and Tools, 2.4 Given a scenario, use appropriate tools and techniques to troubleshoot security issues, p. 21

NEW QUESTION 17
- (Exam Topic 1)
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

A. Disable unneeded services.
B. Install the latest security patches.
C. Run a vulnerability scan.
D. Encrypt all disks.

Answer: C

Explanation:
Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3

NEW QUESTION 18
- (Exam Topic 1)
A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

A. Security patches were uninstalled due to user impact.
B. An adversary altered the vulnerability scan reports
C. A zero-day vulnerability was used to exploit the web server
D. The scan reported a false negative for the vulnerability

Answer: A

Explanation:
A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications.
If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.
The other options are not correct because:
➢ B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.
➢ C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.
➢ D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.
According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:
“A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers.”
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/

NEW QUESTION 19
- (Exam Topic 1)
A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted Which of the following is the researcher MOST likely using?

A. The Cyber Kill Chain
B. The incident response process
C. The Diamond Model of Intrusion Analysis
D. MITRE ATT&CK

Answer: D

Explanation:
The researcher is most likely using the MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations. It helps security teams better understand and track adversaries by creating a named group, which aligns with the scenario described in the question. The framework is widely recognized and referenced in the cybersecurity industry, including in CompTIA Security+ study

materials. References: 1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf 2. MITRE ATT&CK: https://attack.mitre.org/
MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors. MITRE ATT&CK also allows security researchers to create named groups that track specific adversaries based on their TTPs.
The other options are not correct because:

- A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.
- B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.
- C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.

According to CompTIA Security+ SY0-601 Exam Objectives 1.1 Compare and contrast different types of social engineering techniques:
“MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors.”
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://attack.mitre.org/

NEW QUESTION 24
- (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 29
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framevtoik
D. ISO 27002

Answer: C

Explanation:
The CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system. The RMF is a structured process for managing risks that involves categorizing the system, selecting controls, implementing controls, assessing controls, and authorizing the system.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 4: Risk Management, pp. 188-191.

NEW QUESTION 33
- (Exam Topic 1)
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework

Answer: B

Explanation:
The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:

- CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.
- CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

NEW QUESTION 36
- (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 39
- (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 40
- (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 43
- (Exam Topic 1)
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable
To improve security? (Select TWO.)

A. RADIUS
B. PEAP
C. WPS
D. WEP-EKIP
E. SSL
F. WPA2-PSK

Answer: AF

Explanation:
To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

NEW QUESTION 47
- (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?

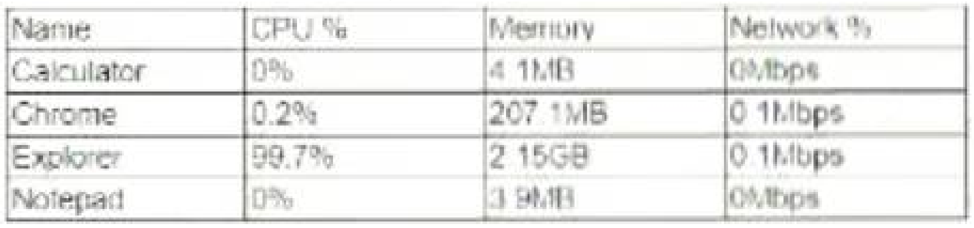
A. openssl
B. hping
C. netcat
D. tcpdump

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 48
- (Exam Topic 1)
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results



Name	CPU %	Memory	Network %
Calculator	0%	4 1MB	0Mbps
Chrome	0.2%	207 1MB	0 1Mbps
Explorer	99.7%	2 15GB	0 1Mbps
Notepad	0%	3 9MB	0Mbps

Which of the following is MOST likely the issue?

A. RAT
B. PUP
C. Spyware
D. Keylogger

Answer: C

Explanation:
Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:
- CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
- CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 50
- (Exam Topic 1)
A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming
B. Port mirroring
C. Defense in depth
D. High availability
E. Geographic dispersal

Answer: C

Explanation:
Defense in depth is a resiliency technique that involves implementing multiple layers of security controls to protect against different types of threats. In this scenario, the NIPS likely provided protection at a different layer than the boundary firewall, demonstrating the effectiveness of defense in depth. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 51
- (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 54
- (Exam Topic 1)
A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?

A. A service-level agreement
B. A business partnership agreement
C. A SOC 2 Type 2 report
D. A memorandum of understanding

Answer: C

Explanation:
SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.
A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess

the vendor's security posture despite the vendor not allowing for a direct audit.
The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

NEW QUESTION 57
- (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 59
- (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 63
- (Exam Topic 1)
The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

A. prepending.
B. an influence campaign.
C. a watering-hole attack.
D. intimidation.
E. information elicitation.

Answer: B

Explanation:
This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

NEW QUESTION 68
- (Exam Topic 1)
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions 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 nsk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules,
C. Emulate the malware in a heavily monitored DMZ segment
D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:
Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques. References: CompTIA Security+ Study Guide, page 129

NEW QUESTION 73
- (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 77
- (Exam Topic 1)
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images
B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
C. Define a vulnerability scan to assess container images before being introduced on the environment
D. Create a dedicated VPC for the containerized environment

Answer: A

Explanation:
Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 11: Cloud Security, Container Security

NEW QUESTION 80
- (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:
Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 1: Attacks, Threats, and Vulnerabilities

NEW QUESTION 81
- (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 83
- (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 85
- (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 90
- (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 https://;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 94
- (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?

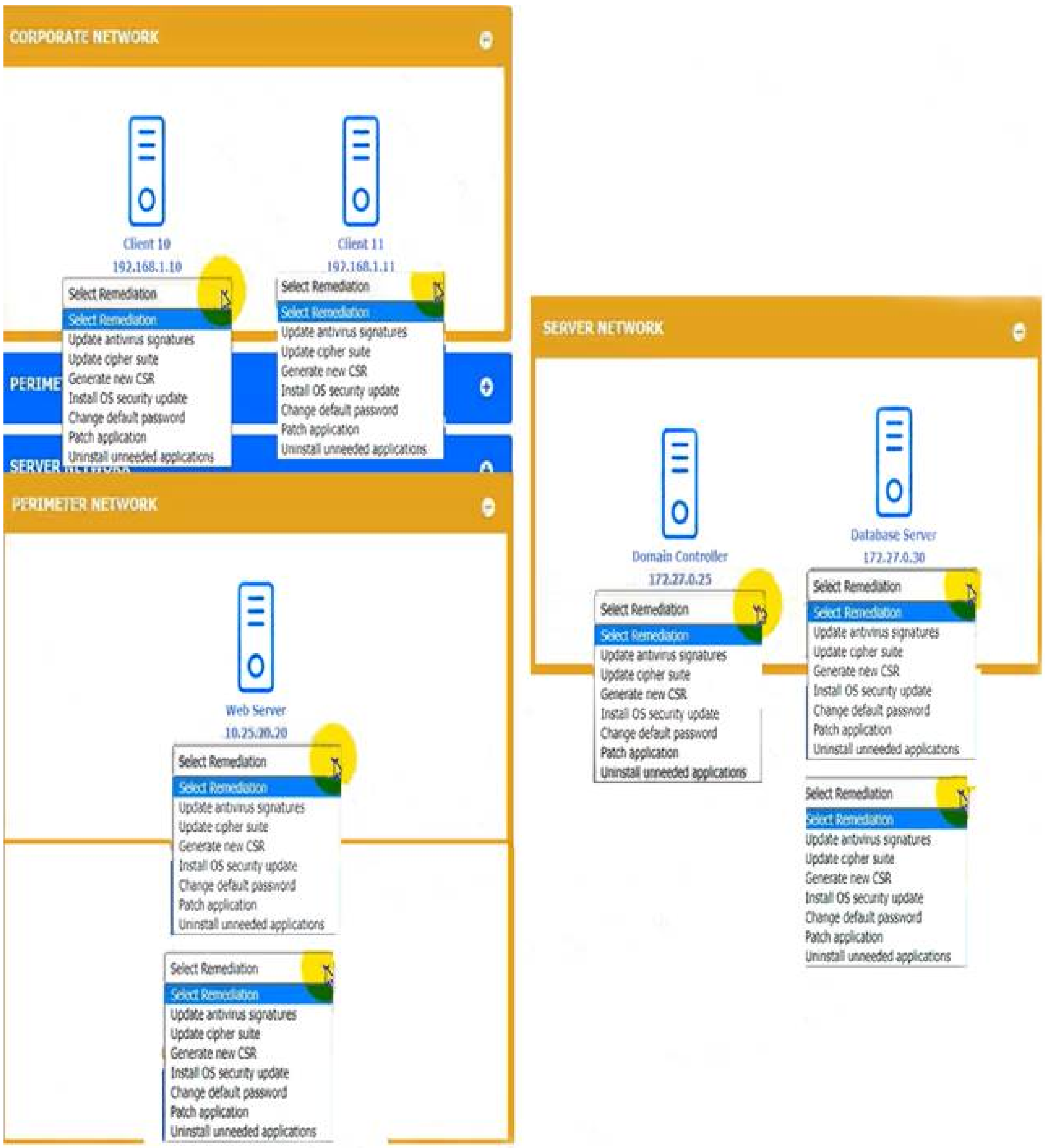
A. Authentication protocol
B. Encryption type
C. WAP placement
D. VPN configuration

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.

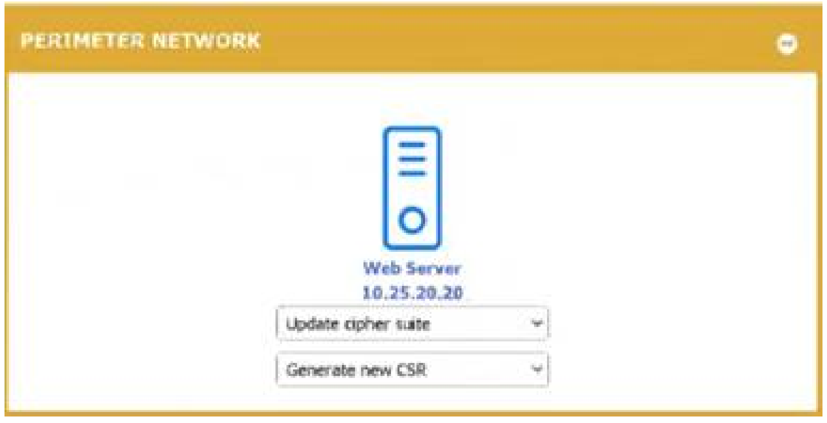
NEW QUESTION 99
- (Exam Topic 1)
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce. Remediation options may be selected multiple times, and some devices may require more than one
remediation.
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

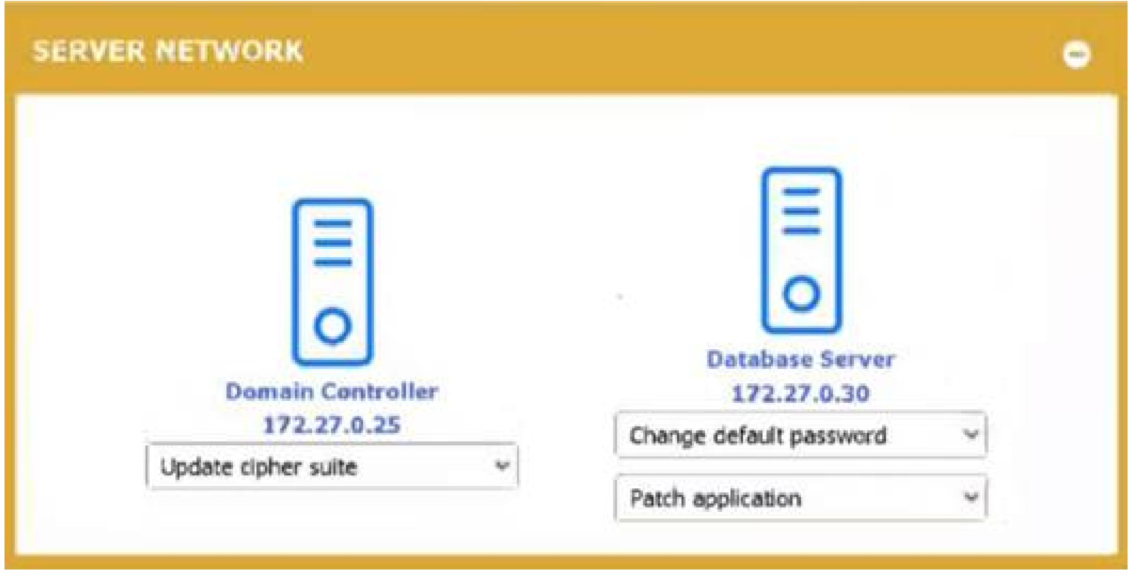
Answer: A

Explanation:


PERIMETER NETWORK

Web Server
10.25.20.20
Update cipher suite
Generate new CSR

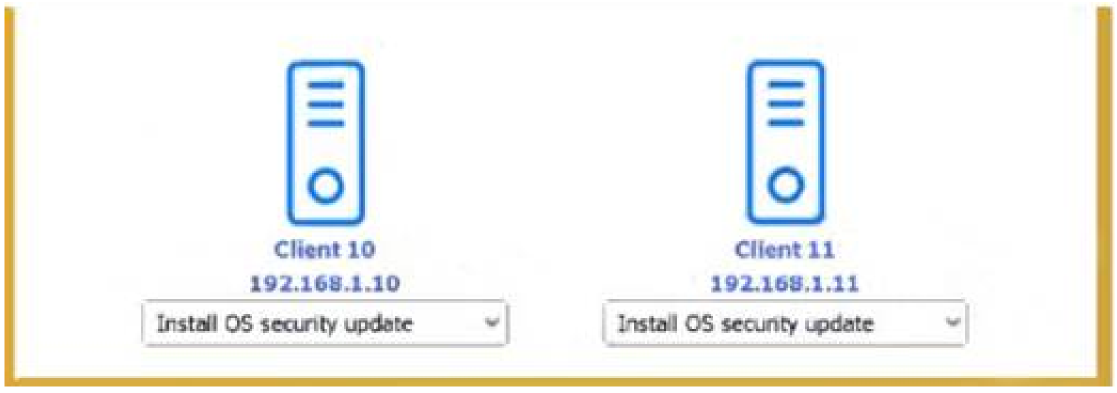
Graphical user interface, application, website, Teams Description automatically generated


SERVER NETWORK

Domain Controller
172.27.0.25
Update cipher suite

Database Server
172.27.0.30
Change default password
Patch application

Graphical user interface, text, application Description automatically generated



NEW QUESTION 103
- (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 108
- (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 113
- (Exam Topic 1)
Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE
B. TPM
C. HIDS
D. VPN

Answer: A

Explanation:
Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE123. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data3. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

NEW QUESTION 118
- (Exam Topic 1)
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII

B. TLP
C. TTP
D. STIX

Answer: A

Explanation:
Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner. References: CompTIA Security+ Certification Exam Objectives 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

NEW QUESTION 121
- (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 124
- (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 126
- (Exam Topic 2)
A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are
being transmitted and stored more securely?

A. Blockchain
B. Salting
C. Quantum
D. Digital signature

Answer: B

Explanation:
Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.
A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION 127
- (Exam Topic 2)

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

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

Answer: C

Explanation:
Jailbreaking is the vulnerability that the organization is addressing by adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Jailbreaking is the process of removing the restrictions or limitations imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking can allow users to install unauthorized applications, customize settings, or access system files. However, jailbreaking can also expose the device to security risks, such as malware, data loss, or warranty voidance. References: https://www.comptia.org/blog/what-is-jailbreaking
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 128
- (Exam Topic 2)
An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack
B. Protocol poisoning
C. Domain hijacking
D. Bluejacking

Answer: A

Explanation:
An on-path attack is an attack that took place when an attacker was eavesdropping on a user who was shopping online and was able to spoof the IP address associated with the shopping site. An on-path attack is a type of network attack that involves intercepting or modifying traffic between two parties by placing oneself in the communication path. An on-path attack can also be called a man-in-the-middle attack or a session hijacking attack. An on-path attacker can steal sensitive information, such as credit card details, or redirect the user to a malicious website. References: https://www.comptia.org/blog/what-is-a-man-in-the-middle-attack
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 132
- (Exam Topic 2)
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

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

Answer: C

Explanation:
Continuous validation is a process that involves performing regular and automated tests to verify the security and functionality of a system or an application. Continuous validation can help identify and remediate vulnerabilities, bugs, or misconfigurations before they cause any damage or disruption. The security administrator’s activities of performing weekly vulnerability scans on all cloud assets and providing a detailed report are examples of continuous validation.

NEW QUESTION 136
- (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 140
- (Exam Topic 2)
An organization wants to quickly assess how effectively the IT team hardened new laptops Which of the following would be the best solution to perform this assessment?

A. Install a SIEM tool and properly configure it to read the OS configuration files.
B. Load current baselines into the existing vulnerability scanner.
C. Maintain a risk register with each security control marked as compliant or non-compliant.
D. Manually review the secure configuration guide checklists.

Answer: B

Explanation:
A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses. This is a quick and automated way to assess the hardening of the new laptops.

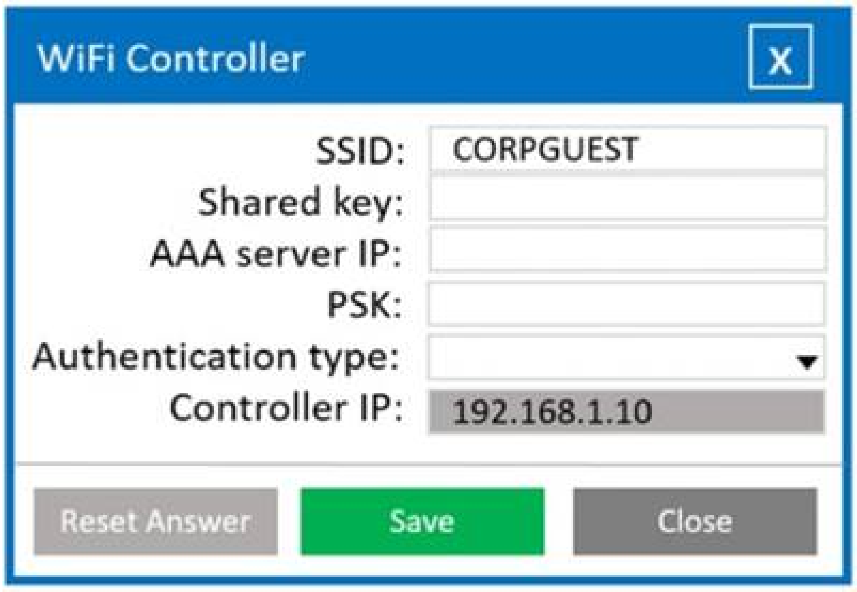
NEW QUESTION 141
- (Exam Topic 2)
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. laaS
D. DaaS

Answer: C

Explanation:
laaS (Infrastructure as a Service) is a cloud model that provides clients with servers, storage, and networks but nothing else. It allows clients to have more control and flexibility over the configuration and management of their infrastructure resources, but also requires them to install and maintain their own operating systems, applications, etc.

NEW QUESTION 142
- (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



WiFi Controller

SSID: CORPGUEST
Shared key:
AAA server IP:
PSK:
Authentication type:
Controller IP: 192.168.1.10

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 143
- (Exam Topic 2)
A technician is setting up a new firewall on a network segment to allow web traffic to the internet while hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

A. Setting an explicit deny to all traffic using port 80 instead of 443

B. Moving the implicit deny from the bottom of the rule set to the top
C. Configuring the first line in the rule set to allow all traffic
D. Ensuring that port 53 has been explicitly allowed in the rule set

Answer: D

Explanation:
Port 53 is the default port for DNS traffic. If the firewall is blocking port 53, then users will not be able to resolve domain names and will receive errors stating that the website could not be located.
The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic. Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.
Therefore, the best way to correct the issue is to ensure that port 53 has been explicitly allowed in the rule set. Here are some additional information about DNS traffic:

- DNS traffic is used to resolve domain names to IP addresses.
- DNS traffic is typically unencrypted, which makes it vulnerable to eavesdropping.
- There are a number of ways to secure DNS traffic, such as using DNS over HTTPS (DoH) or DNS over TLS (DoT).

NEW QUESTION 147
- (Exam Topic 2)
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:
GET
http://yourbank.com/transfer.do?acctnum=08764 6959
&amount=500000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646958
&amount=5000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=-087646958
&amount=1000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646953
&amount=500 HTTP/1.1
Which of the following types of attacks is most likely being conducted?

A. SQLi
B. CSRF
C. Spear phishing
D. API

Answer: B

Explanation:
CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated1. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user's session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.
* A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution2. The output of the web server log does not show any SQL statements or commands.
* B. CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials1. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.
* C. Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email or message that contains a malicious link or attachment3. The output of the web server log does not show any email or message content or headers.
* D. API. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API is not an attack method, but rather a way of designing and developing software applications.

NEW QUESTION 150
- (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 152

- (Exam Topic 2)
A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls

Answer: C

Explanation:
Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.
In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:

- Encrypting data on removable media
- Scanning removable media for malware before use
- Restricting access to removable media ports
- Implementing policies and procedures for removable media usage and disposal
- Educating users on the risks and best practices of removable media

NEW QUESTION 155
- (Exam Topic 2)
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate data center that houses confidential information There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself Which of the following is the weakest design element?

A. The DLP appliance should be integrated into a NGFW.
B. Split-tunnel connections can negatively impact the DLP appliance's performance.
C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

Explanation:
VPN (Virtual Private Network) traffic is encrypted to protect its confidentiality and integrity over the internet. However, this also means that it cannot be inspected by security devices or tools when entering or leaving the network, unless it is decrypted first. This can create a blind spot or a vulnerability for the network security posture, as malicious traffic or data could bypass detection or prevention mechanisms by using VPN encryption

NEW QUESTION 159
- (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 163
- (Exam Topic 2)
A data cento has experienced an increase in under-voltage events Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability Which of the following would be the most cost-effective solution for the data center 10 implement"

A. Uninterruptible power supplies with battery backup
B. Managed power distribution units lo track these events
C. A generator to ensure consistent, normalized power delivery
D. Dual power supplies to distribute the load more evenly

Answer: A

Explanation:
Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events

following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes. References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.apc.com/us/en/faqs/FA158852/

NEW QUESTION 166
- (Exam Topic 2)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

A. MFA
B. Lockout
C. Time-based logins
D. Password history

Answer: A

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user’s identity using two or more
factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:

- https://www.comptia.org/certifications/security
- https://www.youtube.com/watch?v=yCJyPPvM-xg
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/

NEW QUESTION 171
- (Exam Topic 2)
Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

A. User
B. Wildcard
C. Self-signed
D. Root

Answer: B

Explanation:
A wildcard certificate is a type of digital certificate that can be used to secure multiple subdomains under a single domain name. For example, a wildcard certificate for *.example.com can be used to secure www.example.com, mail.example.com, blog.example.com, etc. A wildcard certificate can make administration easier by reducing the number of certificates that need to be issued, managed, and renewed. It can also save costs and simplify configuration.

NEW QUESTION 172
- (Exam Topic 2)
Security analysts notice a server login from a user who has been on vacation for two weeks, The an-alysts confirm that the user did not log in to the system while on vacation After reviewing packet capture the analysts notice the following:
Which of the following occurred?

A. A buffer overflow was exploited to gain unauthorized access.
B. The user's account was con-promised, and an attacker changed the login credentials.
C. An attacker used a pass-the-hash attack to gain access.
D. An insider threat with username logged in to the account.

Answer: C

Explanation:
A pass-the-hash attack is a type of replay attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is possible be-cause some authentication protocols send hashes over the network instead of plain text passwords. The packet capture shows that the attacker used NTLM authentication, which is vulnerable to pass-the-hash attacks

NEW QUESTION 174
- (Exam Topic 2)
A new security engineer has started hardening systems. One o(the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability lo use SCP to transfer files to the NAS, even though the data is still viewable from the users' 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.conf instead of using the ssh
D. conf.
E. Network services are no longer running on the NAS

Answer: B

Explanation:

SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 176
- (Exam Topic 2)
A malicious actor recently penetrated a company's network and moved laterally to the data center Upon investigation a forensics firm wants to know what was in the memory on the compromised server Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

Explanation:
A dump file is a file that contains the contents of memory at a specific point in time. It can be used for debugging or forensic analysis of a system or an application. It can reveal what was in the memory on the compromised server, such as processes, variables, passwords, encryption keys, etc.

NEW QUESTION 179
- (Exam Topic 2)
A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

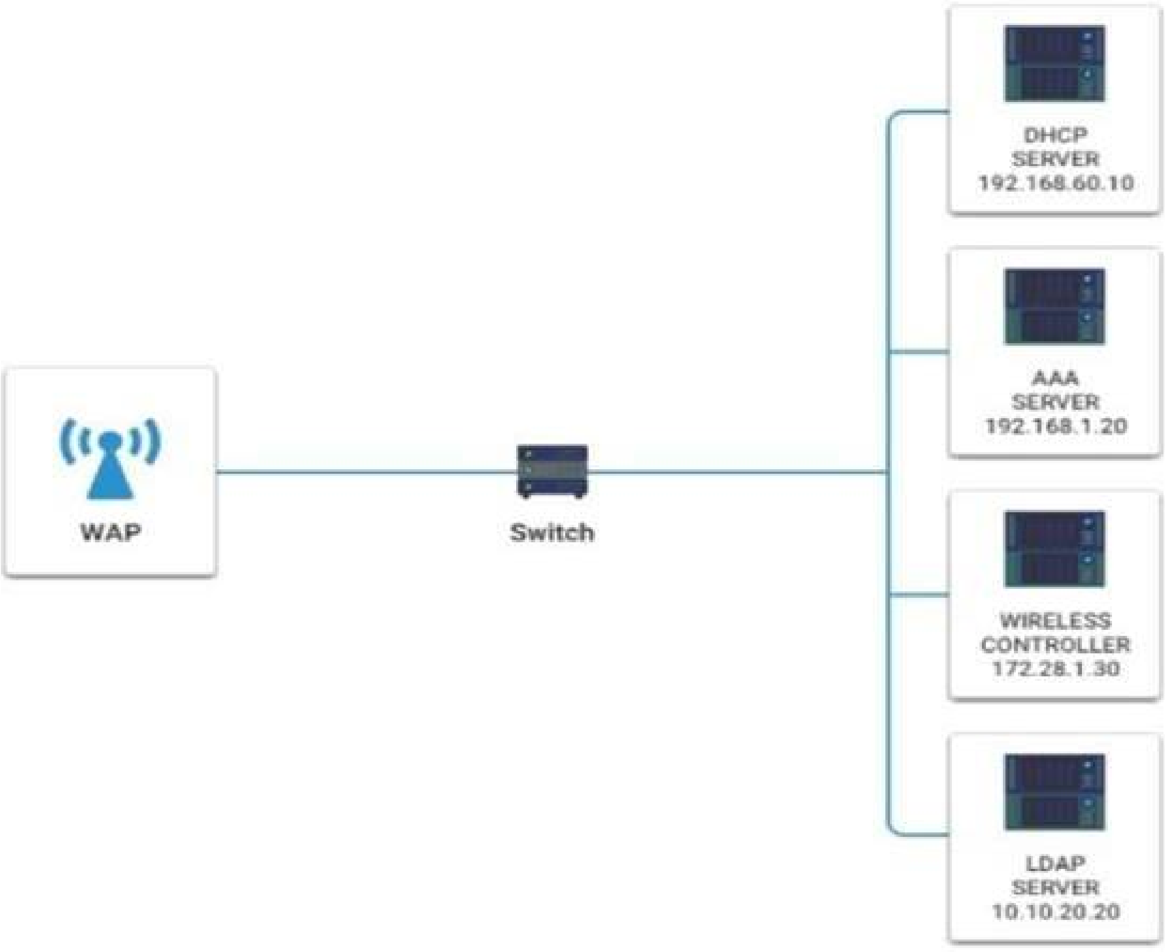
A. Application management
B. Content management
C. Containerization
D. Full disk encryption

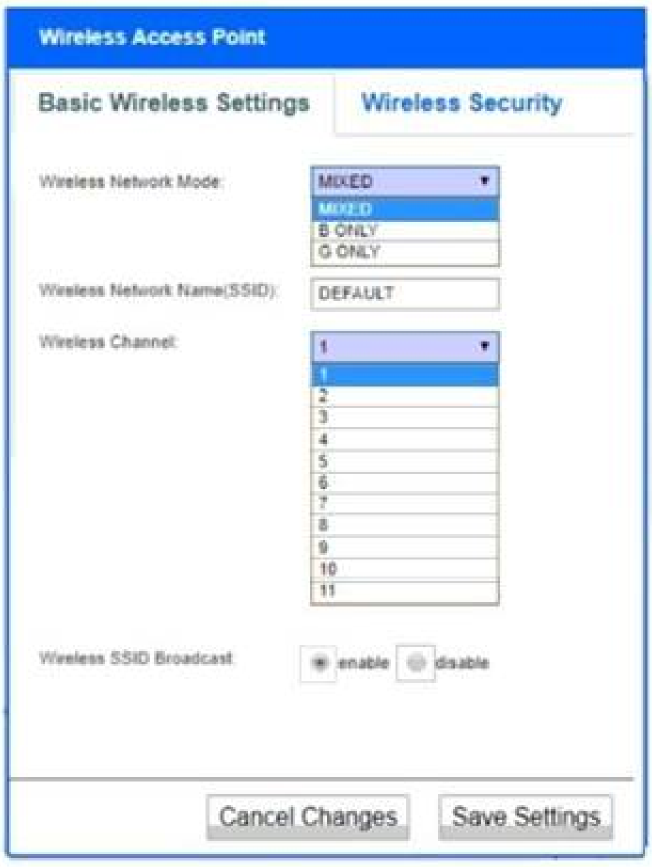
Answer: B

Explanation:
Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.
References: 1
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and
Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA
Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement
secure network architecture concepts 3 https://www.comptia.org/blog/what-is-data-loss-prevention

NEW QUESTION 184
- (Exam Topic 2)
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS
Please click on the below items on the network diagram and configure them accordingly:
- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server

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




Wireless Access Point

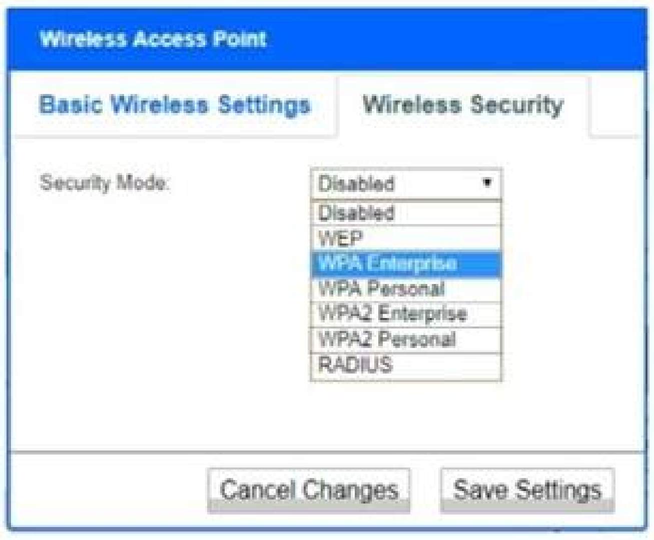
Basic Wireless Settings | Wireless Security

Wireless Network Mode: MIXED

Wireless Network Name(SSID): DEFAULT

Wireless Channel: 1

Wireless SSID Broadcast: ● enable ○ disable


Wireless Access Point

Basic Wireless Settings | Wireless Security

Security Mode: Disabled

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Wireless Access Point Network Mode – G only Wireless Channel – 11
Wireless SSID Broadcast – disable Security settings – WPA2 Professional

NEW QUESTION 186
- (Exam Topic 2)
Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation

Answer: A

Explanation:
A full inventory of all hardware and software would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed, as it would allow the analyst to identify which systems and applications are affected by the vulnerability and prioritize the remediation efforts accordingly. A full inventory would also help the analyst to determine the impact and likelihood of a successful exploit, as well as the potential loss of confidentiality, integrity and availability of the data and services. References:
> https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/risk-analysis/

- https://www.comptia.org/landing/securityplus/index.html
- https://www.comptia.org/blog/complete-guide-to-risk-management

NEW QUESTION 191
- (Exam Topic 2)
A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.
Which of the following should the security operations center implement?

A. theHarvester
B. Nessus
C. Cuckoo
D. Sn1per

Answer: C

Explanation:
Cuckoo is a sandbox that is specifically written to run programs inside and identify any malware. A sandbox is a virtualized environment that isolates the program from the rest of the system and monitors its behavior. Cuckoo can analyze files of various types, such as executables, documents, URLs, and more. Cuckoo can provide a report of the files' activity against known threats, such as network traffic, file operations, registry changes, API calls, and so on.
A security operations center can implement Cuckoo to execute files to test for malicious activity and generate a report of the analysis. Cuckoo can help the security operations center to detect and prevent malware infections, investigate incidents, and perform threat intelligence.

NEW QUESTION 193
- (Exam Topic 2)
A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1.
Which of the following would provide this information?

A. cat /var/messages | grep 10.1.1.1
B. grep 10.1.1.1 | cat /var/messages
C. grep /var/messages | cat 10.1.1.1
D. cat 10.1.1.1 | grep /var/messages

Answer: A

Explanation:
the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

NEW QUESTION 197
- (Exam Topic 2)
Which Of the following is the best method for ensuring non-repudiation?

A. SSO
B. Digital certificate
C. Token
D. SSH key

Answer: B

Explanation:
A digital certificate is an electronic document that contains the public key and identity information of an entity, such as a person, organization, website, etc. It is issued and signed by a trusted authority called a certificate authority (CA). It can provide non-repudiation by proving the identity and authenticity of the sender and verifying the integrity of the message or data.

NEW QUESTION 201
- (Exam Topic 2)
Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

A. Memory, disk, temporary filesystems, CPU cache
B. CPU cache, memory, disk, temporary filesystems
C. CPU cache, memory, temporary filesystems, disk
D. CPU cache, temporary filesystems, memory, disk

Answer: C

Explanation:
The correct order of evidence from most to least volatile in forensic analysis is based on how quickly the evidence can be lost or altered if not collected or preserved properly. CPU cache is the most volatile type of evidence because it is stored in a small amount of memory on the processor and can be overwritten or erased very quickly. Memory is the next most volatile type of evidence because it is stored in RAM and can be lost when the system is powered off or rebooted. Temporary filesystems are less volatile than memory because they are stored on disk, but they can still be deleted or overwritten by other processes or users. Disk is the least volatile type of evidence because it is stored on permanent storage devices and can be recovered even after deletion or formatting, unless overwritten by new data. References:
https://www.comptia.org/blog/what-is-volatility-in-digital-forensics

NEW QUESTION 202
- (Exam Topic 2)

An audit identified Pll being utilized in the development environment of a crit-ical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed: however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to best satisfy both the CPOs and the development team's requirements?

A. Data purge
B. Data encryption
C. Data masking
D. Data tokenization

Answer: D

Explanation:
Data tokenization is a technique of replacing sensitive data with non-sensitive substitutes called tokens that have no intrinsic value or meaning. It can satisfy both the CPO's and the development team's requirements by removing personally identifiable information (PII) from the development environment of a critical application while preserving the functionality and format of the data for testing purposes.

NEW QUESTION 205
- (Exam Topic 2)
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

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

Answer: B

Explanation:
Testing the policy in a non-production environment before enabling the policy in the production network would prevent the issue of making several company servers unreachable. A non-production environment is a replica of the production network that is used for testing, development, or training purposes. By testing the policy in a non-production environment, the technician can verify the functionality and impact of the policy without affecting the real network or users. This can help to identify and resolve any errors or conflicts before applying the policy to the production network. Testing the policy in a non-production environment can also help to ensure compliance with security standards and best practices.

NEW QUESTION 208
- (Exam Topic 2)
Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan

Answer: B

Explanation:
A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented.

NEW QUESTION 212
- (Exam Topic 2)
A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

A. DLP
B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF

Answer: CD

Explanation:
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

NEW QUESTION 217
- (Exam Topic 2)
An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

A. a push notification

B. a password.
C. an SMS message.
D. an authentication application.

Answer: D

Explanation:
An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

NEW QUESTION 218
- (Exam Topic 2)
The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

A. HIDS
B. FDE
C. NGFW
D. EDR

Answer: D

Explanation:
EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

NEW QUESTION 221
- (Exam Topic 2)
A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

A. Dump file
B. System log
C. Web application log
D. Security too

Answer: A

Explanation:
A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files

NEW QUESTION 222
- (Exam Topic 2)
A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner, Which of the following concepts describes this scenario?

A. Red-team exercise
B. Business continuity plan testing
C. Tabletop exercise
D. Functional exercise

Answer: C

Explanation:
A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it1. A tabletop exercise is a low-impact and
cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and
enhance communication and coordination among team members2. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization3. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption4. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.
References: 1:
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g
2: https://www.linuxjournal.com/content/security-exercises 3:
https://www.imperva.com/learn/application-security/red-team-blue-team/ 4: https://www.ready.gov/business-continuity-plan : https://www.ready.gov/exercises

NEW QUESTION 223
- (Exam Topic 2)
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

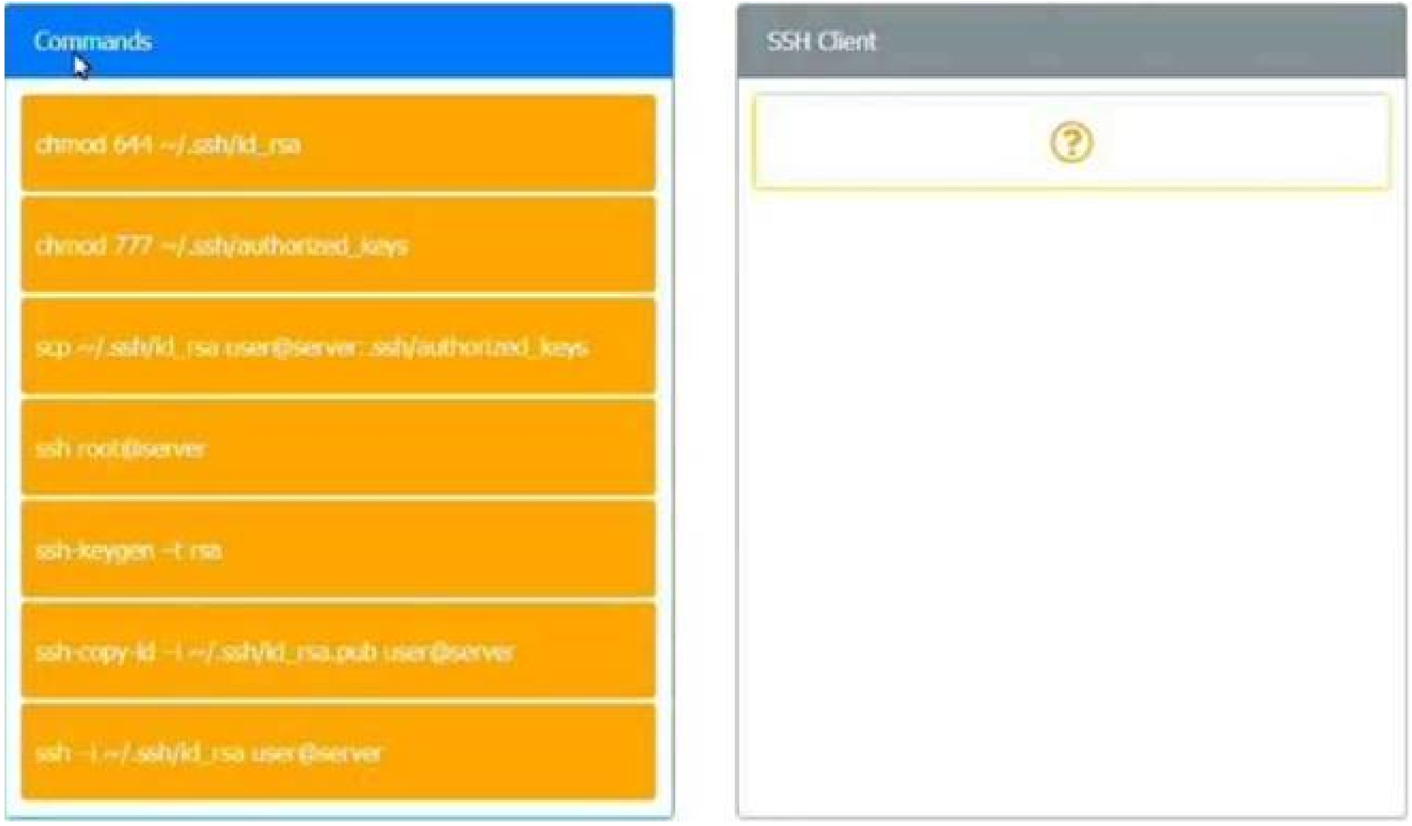
A. Always-on
B. Remote access
C. Site-to-site
D. Full tunnel

Answer: C

Explanation:
Site-to-site VPN is a type of VPN solution that connects two or more networks or sites across the public internet in a secure and encrypted way. Site-to-site VPN can be implemented using VPN appliances, such as firewalls or routers, that can establish and maintain the VPN tunnel between the sites. Site-to-site VPN can support multiple users or devices that need to access resources on the other site without requiring individual VPN clients or software. Site-to-site VPN is the best solution to support the new remote office, as it can provide secure and seamless connectivity between the office network and the main network of the organization.
Verified References:

- Virtual Private Networks – SY0-601 CompTIA Security+ : 3.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/virtual-private-networks-sy0-601- (See Site-to-Site VPN)
- VPN Technologies – CompTIA Security+ SY0-501 – 3.2 https://www.professormesser.com/security-plus/sy0-501/vpn-technologies/ (See Site-to-Site VPN)
- Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.3: Given a scenario, implement secure network architecture concepts.)

NEW QUESTION 224
- (Exam Topic 2)
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
chmod 644 ~/.ssh/id_rsa
chmod 777 ~/.ssh/authorized_keys
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys
ssh root@server
ssh-keygen –t rsa
ssh-copy-id –i ~/.ssh/id_rsa.pub user@server
ssh –i ~/.ssh/id_rsa user@server
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 228
- (Exam Topic 2)
An organization is repairing damage after an incident. Which Of the following controls is being implemented?

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

Answer: C

Explanation:
Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

NEW QUESTION 230
- (Exam Topic 2)
An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

A. Intrusion prevention system

B. Proxy server
C. Jump server
D. Security zones

Answer: A

Explanation:
An intrusion prevention system (IPS) is the best solution to implement on the company's network to detect and prevent suspicious attempts to access company resources. An IPS is a network security technology that continuously monitors network traffic for malicious or anomalous activity and takes automated actions to block or mitigate it. An IPS can also alert the system administrators of any potential threats and provide detailed logs and reports of the incidents. An IPS can help the company to improve its security posture and prevent data breaches, unauthorized access, or denial-of-service attacks. References:

- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

NEW QUESTION 232
- (Exam Topic 2)
A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?

A. DLP
B. SIEM
C. NIDS
D. WAF

Answer: D

Explanation:
WAF stands for Web Application Firewall, which is a type of firewall that can monitor, filter and block web traffic to and from web applications. WAF can protect web applications from common attacks such as
cross-site scripting (XSS), SQL injection, directory traversal, buffer overflow and more. WAF can also enforce security policies and rules that can prevent parameter manipulation or tampering by an unknown third party. WAF is the best solution to help protect against the attack on the web API, as it can inspect the HTTP requests and responses and block any malicious or anomalous activity. Verified References:

- Other Application Attacks – SY0-601 CompTIA Security+ : 1.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/other-application-attacks/ (See Web Application Firewall)
- CompTIA Security+ SY0-601 Exam Cram
https://www.oreilly.com/library/view/comptia-security-sy0-601/9780136798767/ch03.xhtml (See Web Application Firewall)
- Security+ domain #1: Attacks, threats, and vulnerabilities [updated 2021] https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/ (See Web application firewall)

NEW QUESTION 236
- (Exam Topic 2)
A company needs to enhance Its ability to maintain a scalable cloud Infrastructure. The Infrastructure needs to handle the unpredictable loads on the company's web application. Which of the following
cloud concepts would BEST these requirements?

A. SaaS
B. VDI
C. Containers
D. Microservices

Answer: C

Explanation:
Containers are a type of virtualization technology that allow applications to run in a secure, isolated environment on a single host. They can be quickly scaled up or down as needed, making them an ideal solution for unpredictable loads. Additionally, containers are designed to be lightweight and portable, so they can easily be moved from one host to another. Reference: CompTIA Security+ Sy0-601 official Text book, page 863.

NEW QUESTION 238
- (Exam Topic 2)
Employees in the research and development business unit receive extensive training 10 ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit

Answer: B

Explanation:
Intellectual property is a type of data that is proprietary and unique to an organization. It includes trade secrets and other information that the organization does not want to share with third parties or competitors. Employees in the research and development business unit are most likely to use intellectual property in their day-to-day work activities, as they are involved in creating new products, services, or processes for the organization. Intellectual property data requires a high level of security and protection, as it can provide a competitive advantage or disadvantage if leaked or stolen.
Encrypted data is not a type of data, but a state of data. Encryption is a method of transforming data into an unreadable format using a key, so that only authorized parties can access it. Encryption can be applied to any type of data, such as intellectual property, critical data, or data in transit.
Critical data is a type of data that is essential for the operation and continuity of an organization. It includes information such as customer records, financial transactions, employee details, and so on. Critical data may or may not be intellectual property, depending on the nature and source of the data. Critical data also requires a high level of security and protection, as it can affect the reputation, performance, or legal compliance of the organization.

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

NEW QUESTION 243
- (Exam Topic 2)
A security administrator is managing administrative access to sensitive systems with the following requirements:
• Common login accounts must not be used for administrative duties.
• Administrative accounts must be temporal in nature.
• Each administrative account must be assigned to one specific user.
• Accounts must have complex passwords.
" Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements? (Give explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

A. ABAC
B. SAML
C. PAM
D. CASB

Answer: C

Explanation:
PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, “PAM is the most comprehensive way to control and monitor privileged accounts”.

NEW QUESTION 246
- (Exam Topic 2)
A security analyst reviews web server logs and notices the following line: 104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072
http://www.example.com/wordpress/wp—admin/
Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF
B. CSRF
C. xss
D. SQLi

Answer: D

Explanation:
SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.
The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users’ accounts.

NEW QUESTION 250
- (Exam Topic 2)
Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

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

Answer: D

Explanation:
AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company’s IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity1.
https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/ 3:
https://www.professormesser.com/security-plus/sy0-501/agreement-types/ 1: https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

NEW QUESTION 252
- (Exam Topic 2)
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

A. Time stamp
B. Chain of custody
C. Admissibility
D. Legal hold

Answer: B

Explanation:
Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.thoughtco.com/chain-of-custody-4589132

NEW QUESTION 255
- (Exam Topic 2)
A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor. Which of the following authentication methods should the systems administrator choose? (Select two).

A. passphrase
B. Time-based one-time password
C. Facial recognition
D. Retina scan
E. Hardware token
F. Fingerprints

Answer: BE

Explanation:
Time-based one-time password (TOTP) and hardware token are authentication methods that rely on the possession factor, which means that the user must have a specific device or object in their possession to authenticate. A TOTP is a password that is valid for a short period of time and is generated by an app or a device that the user has. A hardware token is a physical device that displays a code or a password that the user can enter to authenticate. A passphrase (Option A) is a knowledge factor, while facial recognition (Option C), retina scan (Option D), and fingerprints (Option F) are all inherence factors.
https://ptgmedia.pearsoncmg.com/imprint_downloads/pearsonitcertification/bookreg/9780136798675/97801367 https://www.youtube.com/watch?v=yCJyPPvM-xg

NEW QUESTION 259
- (Exam Topic 2)
A web architect would like to move a company's website presence to the cloud. One of the management team's key concerns is resiliency in case a cloud provider's data center or network connection goes down. Which of the following should the web architect consider to address this concern?

A. Containers
B. Virtual private cloud
C. Segmentation
D. Availability zones

Answer: D

Explanation:
Availability zones are the most appropriate cloud feature to address the concern of resiliency in case a cloud provider’s data center or network connection goes down. Availability zones are physically separate locations within an Azure region that have independent power, cooling, and networking. Each availability zone is made up of one or more data centers and houses infrastructure to support highly available, mission-critical applications. Availability zones are connected with high-speed, private fiber-optic networks. Azure services that support availability zones fall into two categories: Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses), or Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database). To achieve comprehensive business continuity on Azure, build your application architecture using the combination of availability zones with Azure region pairs. You can synchronously replicate your applications and data using availability zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.

NEW QUESTION 261
- (Exam Topic 2)
A company has installed badge readers for building access but is finding unau-thorized individuals roaming the hallways Of the following is the most likely cause?

A. Shoulder surfing
B. Phishing
C. Tailgating
D. Identity fraud

Answer: C

Explanation:
Tailgating is a physical security threat that occurs when an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. It can cause unauthorized individuals to roam the hallways after gaining access through badge readers installed for building access.

NEW QUESTION 262
- (Exam Topic 2)
A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framework
D. ISO 27002

Answer: C

Explanation:

The NIST Risk Management Framework (RMF) is a process for evaluating the security of a system and implementing controls to reduce potential risks associated with it. The RMF process involves categorizing the system, selecting the controls that apply to the system, implementing the controls, and then assessing the success of the controls before authorizing the system. For more information on the NIST Risk Management Framework and other security processes, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 264
- (Exam Topic 2)
A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

A. theHarvester
B. Cuckoo
C. Nmap
D. Nessus

Answer: A

Explanation:
TheHarvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. TheHarvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

NEW QUESTION 267
- (Exam Topic 2)
Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE
B. CVSS
C. CIA
D. CERT

Answer: B

Explanation:
The correct answer is B. CVSS.
CVSS stands for Common Vulnerability Scoring System. It is a framework that provides a standardized way to measure the criticality of a vulnerability based on various factors, such as the impact, exploitability, and remediation level of the vulnerability. CVSS assigns a numerical score from 0 to 10 to each vulnerability, where 0 means no risk and 10 means the highest risk. CVSS also provides a qualitative rating for each score, such as low, medium, high, or critical. CVSS helps organizations prioritize the remediation of vulnerabilities based on their severity and potential impact12.
CVE stands for Common Vulnerabilities and Exposures. It is a list of publicly known and standardized identifiers for vulnerabilities and exposures in software and hardware systems. CVE provides a brief description of each vulnerability or exposure, but does not assign a score or rating to them. CVE helps organizations communicate and share information about vulnerabilities and exposures in a consistent and reliable way3 .
CIA stands for Confidentiality, Integrity, and Availability. It is a model that defines the three main objectives of information security. Confidentiality means protecting data from unauthorized access or disclosure. Integrity means ensuring data is accurate and consistent and has not been tampered with. Availability means ensuring data is accessible and usable by authorized parties when needed. CIA helps organizations design and implement security controls and policies to protect their data and systems .
CERT stands for Computer Emergency Response Team. It is a group of experts who respond to security incidents and provide guidance and assistance to mitigate and prevent cyberattacks. CERT also conducts research and analysis on cybersecurity trends and issues, and disseminates information and best practices to the public. CERT helps organizations improve their security posture and resilience against cyber threats .
For more information on CVSS and other concepts related to vulnerability assessment and management, you can refer to [this video] or [this guide] from CompTIA Security+.

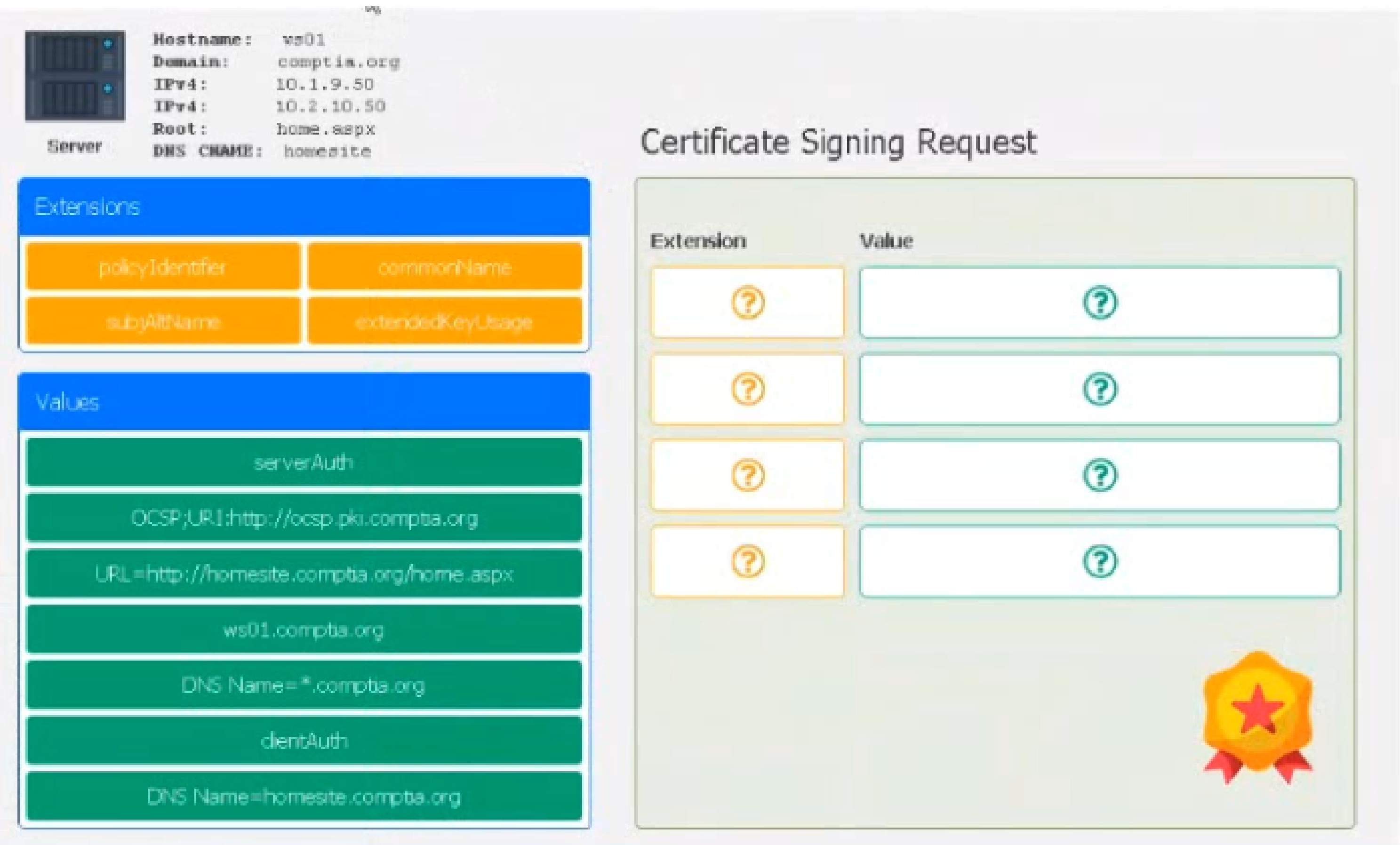
NEW QUESTION 268
- (Exam Topic 2)
Which Of the following supplies non-repudiation during a forensics investiga-tion?

A. Dumping volatile memory contents first
B. Duplicating a drive With dd
C. a SHA 2 signature of a drive image
D. Logging everyone in contact with evidence
E. Encrypting sensitive data

Answer: C

Explanation:
A SHA 2 signature is a cryptographic hash function that produces a unique and fixed-length output for any given input. It can provide non-repudiation during a forensics investigation by verifying the integrity and authenticity of a drive image and proving that it has not been altered or tampered with since it was created

NEW QUESTION 272
- (Exam Topic 2)
Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)
• Hostname: ws01
• Domain: comptia.org
• IPv4: 10.1.9.50
• IPV4: 10.2.10.50
• Root: home.aspx
• DNS CNAME:homesite. Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.



Hostname: ws01
Domain: comptia.org
IPv4: 10.1.9.50
IPv4: 10.2.10.50
Root: home.aspx
DNS CNAME: homesite

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 273
- (Exam Topic 2)
Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan
B. Threat intelligence
C. Log aggregation
D. Packet capture

Answer: D

Explanation:
- Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities
- Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses
- Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling
- Using a CASB tool to control access to cloud resources and prevent data leaks or downloads
- Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

NEW QUESTION 278
- (Exam Topic 2)
A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

A. The vendor firmware lacks support.
B. Zero-day vulnerabilities are being discovered.
C. Third-party applications are not being patched.
D. Code development is being outsourced.

Answer: C

Explanation:
Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

NEW QUESTION 279
- (Exam Topic 2)
A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab The researchers collaborate with other machines using port 445 and on the internet using port 443 The unau-thorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMS. The security team has been instructed to resolve the issue as quickly as possible while causing

minimal disruption to the researchers. Which of the following is the best course Of action in this scenario?

A. Update the host firewalls to block outbound Stv1B.
B. Place the machines with the unapproved software in containment
C. Place the unauthorized application in a Bocklist.
D. Implement a content filter to block the unauthorized software communica-tion,

Answer: B

Explanation:
Containment is an incident response strategy that aims to isolate and prevent the spread of an attack or compromise within a network or system. It can resolve the issue of unauthorized software detected on a small number of machines in a lab as quickly as possible while causing minimal disruption to the researchers by stopping the software from communicating with external sources using HTTPS and SMS and preventing it from infecting additional machines outside of the lab

NEW QUESTION 284
- (Exam Topic 2)
Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

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

Answer: C

Explanation:
The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware. According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

NEW QUESTION 285
- (Exam Topic 2)
A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access pcints are up and running. One of the help desk technicians notices the affected users are working in a near the parking Jot Which Of the following IS the most likely reason for the outage?

A. Someone near the is jamming the signal.
B. A user has set up a rogue access point near building.
C. Someone set up an evil twin access Print in tie affected area.
D. The APS in the affected area have been from the network

Answer: A

Explanation:
Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

NEW QUESTION 286
- (Exam Topic 2)
A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

A. Social media analysis
B. Least privilege
C. Nondisclosure agreements
D. Mandatory vacation

Answer: B

Explanation:
Least privilege is a security principle that states that users and processes should only have the minimum level of access and permissions required to perform their tasks. This reduces the risk of insider threats by limiting the potential damage that a malicious or compromised user or process can cause to the system or data.
References: https://www.comptia.org/blog/what-is-least-privilege

NEW QUESTION 290
- (Exam Topic 2)
Which of the following best describes when an organization Utilizes a read-to-use application from a cloud provider?

A. IaaS
B. SaaS
C. PaaS
D. XaaS

Answer: B

Explanation:
SaaS stands for software as a service, which is a cloud computing model that provides ready-to-use applications over the internet. SaaS applications are hosted and managed by a cloud provider who also handles software updates, maintenance, security, and scalability. SaaS users can access the applications through a web browser or a mobile app without installing any software on their devices. SaaS applications are typically offered on a subscription or pay-per-use basis. Examples of SaaS applications include email services, online office suites, customer relationship management (CRM) systems, and video conferencing platforms. References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ibm.com/cloud/learn/software-as-a-service

NEW QUESTION 293
......