Exam Questions SY0-701

CompTIA Security+ Exam

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

NEW QUESTION 1
- (Exam Topic 1)
A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing
B. Use a web vulnerability scanner
C. Use static code analysis
D. Use a penetration-testing OS

Answer: C

Explanation:
Using static code analysis would be the best approach to scan the source code looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. This method involves analyzing the source code without actually running the software, which can identify security vulnerabilities that may not be detected by other testing methods. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Risk Management, pp. 292-295

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

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

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

Answer: B

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

NEW QUESTION 4
- (Exam Topic 1)
As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops The review yielded the following results.
• The exception process and policy have been correctly followed by the majority of users
• A small number of users did not create tickets for the requests but were granted access
• All access had been approved by supervisors.
• Valid requests for the access sporadically occurred across multiple departments.
• Access, in most cases, had not been removed when it was no longer needed
Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

Answer: A

Explanation:
According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee’s supervisor denies the approval12.
This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

NEW QUESTION 5
- (Exam Topic 1)
Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels

and to measure performance characteristics?

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

Answer: A

Explanation:
The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics. References: CompTIA Security+ Study Guide 601, Chapter 2

NEW QUESTION 6
- (Exam Topic 1)
A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares. Which of the following should the company Implement?

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

Answer: A

Explanation:
The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares. References:
> CompTIA Security+ Study Guide Exam SY0-601, Chapter 8

NEW QUESTION 7
- (Exam Topic 1)
A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

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

Which of the following BEST explains this type of attack?

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

Answer: B

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

NEW QUESTION 8
- (Exam Topic 1)
A security administrator has discovered that workstations on the LAN are becoming infected with malware.
The cause of the infections appears to be users receiving phishing emails that are bypassing the current
email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

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

Answer: C

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

NEW QUESTION 9
- (Exam Topic 1)
A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

A. Privacy
B. Cloud storage of telemetry data
C. GPS spoofing
D. Weather events

Answer: A

Explanation:
The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated. References:
- CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

NEW QUESTION 10
- (Exam Topic 1)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

Answer: A

Explanation:
PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data1. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet1.
One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for2. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org2. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org2.
Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used3. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years3. The validity period can be checked by looking at the valid from and valid to dates on the certificate3.
Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org2. It also has a validity period of one year, which means it needs to be rotated annually3.

NEW QUESTION 10
- (Exam Topic 1)
An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

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

Answer: D

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

NEW QUESTION 12
- (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 13
- (Exam Topic 1)
A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing
B. Phishing

C. Spear phishing
D. Whaling

Answer: A

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

NEW QUESTION 18
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

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

Answer: A

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

NEW QUESTION 23
- (Exam Topic 1)
Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

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

Answer: B

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

NEW QUESTION 24
- (Exam Topic 1)
During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow
B. Pass the hash
C. SQL injection
D. Replay attack

Answer: B

Explanation:
Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user’s password, rather than requiring the plaintext password

NEW QUESTION 27
- (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 31
- (Exam Topic 1)
A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update
B. HTTP headers
C. Secure cookies
D. Third-party updates
E. Full disk encryption
F. Sandboxing
G. Hardware encryption

Answer: AF

Explanation:
Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.
Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary. Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

NEW QUESTION 33
- (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 34
- (Exam Topic 1)
A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:
* Ensure mobile devices can be tracked and wiped.
* Confirm mobile devices are encrypted.
Which of the following should the analyst enable on all the devices to meet these requirements?

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

Answer: A

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

NEW QUESTION 35
- (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 38
- (Exam Topic 1)
Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

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

Answer: D

Explanation:
The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality. References: https://www.techopedia.com/definition/27561/development-environment

NEW QUESTION 42
- (Exam Topic 1)
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

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

Answer: A

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

NEW QUESTION 44
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

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

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-phishing

NEW QUESTION 46
- (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 49
- (Exam Topic 1)
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

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


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

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

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

Answer: B

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

NEW QUESTION 52
- (Exam Topic 1)
A security analyst reviews a company’s authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

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

Answer: C

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

NEW QUESTION 56
- (Exam Topic 1)
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD
B. VDI
C. COPE
D. CYOD

Answer: D

Explanation:
Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices. It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model. References: CompTIA Security+ Study Guide, Chapter 6: Securing Application, Data, and Host Security, 6.5 Implement Mobile Device Management, pp. 334-335

NEW QUESTION 59
- (Exam Topic 1)

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

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

Answer: AD

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

NEW QUESTION 60
- (Exam Topic 1)
During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HIIPS site requests are reverting to HTTP Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key
B. DNS hijacking to reroute traffic
C. Brute force to the access point
D. ASSLILS downgrade

Answer: B

Explanation:
The attendee is experiencing delays in the connection, and the HIIPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.
Reference: https://www.cloudflare.com/learning/dns/dns-hijacking/

NEW QUESTION 64
- (Exam Topic 1)
Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

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

Answer: C

Explanation:
an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspectio3n45, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

NEW QUESTION 65
- (Exam Topic 1)
As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

A. Creating a playbook within the SOAR
B. Implementing rules in the NGFW
C. Updating the DLP hash database
D. Publishing a new CRL with revoked certificates

Answer: A

Explanation:
Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

NEW QUESTION 70
- (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 75
- (Exam Topic 1)
An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

A. Jamming
B. Bluesnarfing
C. Evil twin
D. Rogue access point

Answer: B

Explanation:
Bluesnarfing is a hacking technique that exploits Bluetooth connections to snatch data from a wireless device. An attacker can perform bluesnarfing when the Bluetooth function is on and your device is discoverable by other devices within range. In some cases, attackers can even make calls from their victim’s phon1e.

NEW QUESTION 76
- (Exam Topic 1)
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

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

Answer: A

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

NEW QUESTION 80
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling
B. Spam
C. Invoice scam
D. Pharming

Answer: A

Explanation:
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

NEW QUESTION 84
- (Exam Topic 1)
A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

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

Answer: A

Explanation:
Infrastructure as a Service (IaaS) providers offer a la carte services, including cloud backups, VM elasticity, and secure networking. With IaaS, businesses can rent

infrastructure components such as virtual machines, storage, and networking from a cloud service provider. References: CompTIA Security+ Study Guide, pages 233-234

NEW QUESTION 85
- (Exam Topic 1)
A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:
•Must be able to differentiate between users connected to WiFi
•The encryption keys need to change routinely without interrupting the users or forcing reauthentication
•Must be able to integrate with RADIUS
•Must not have any open SSIDs
Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise
B. WPA3-PSK
C. 802.11n
D. WPS

Answer: A

Explanation:
Detailed
WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication. Additionally, WPA2-Enterprise does not allow for open SSIDs.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7: Securing Networks, p. 317

NEW QUESTION 86
- (Exam Topic 1)
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

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

Answer: B

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

NEW QUESTION 87
- (Exam Topic 1)
Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

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

Answer: C

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

NEW QUESTION 90
- (Exam Topic 1)
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: B

Explanation:

To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 93
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

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

Answer: B

Explanation:
A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION 94
- (Exam Topic 1)
Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management
B. SSO
C. RADIUS
D. Attribute-based access control

Answer: A

Explanation:
The company is implementing privileged access management, which provides just-in-time permissions for administrative functions.

NEW QUESTION 97
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

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

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

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

Answer: C

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

NEW QUESTION 98
- (Exam Topic 1)
Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft
B. Data loss
C. Data exfiltration
D. Reputation

Answer: D

Explanation:

The best option that describes what is impacted the most by the hackers' attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of customers, partners, investors, or employees.

NEW QUESTION 102
- (Exam Topic 1)
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

Answer: A

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

NEW QUESTION 104
- (Exam Topic 1)
An analyst Is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services. Given this output from Nmap:

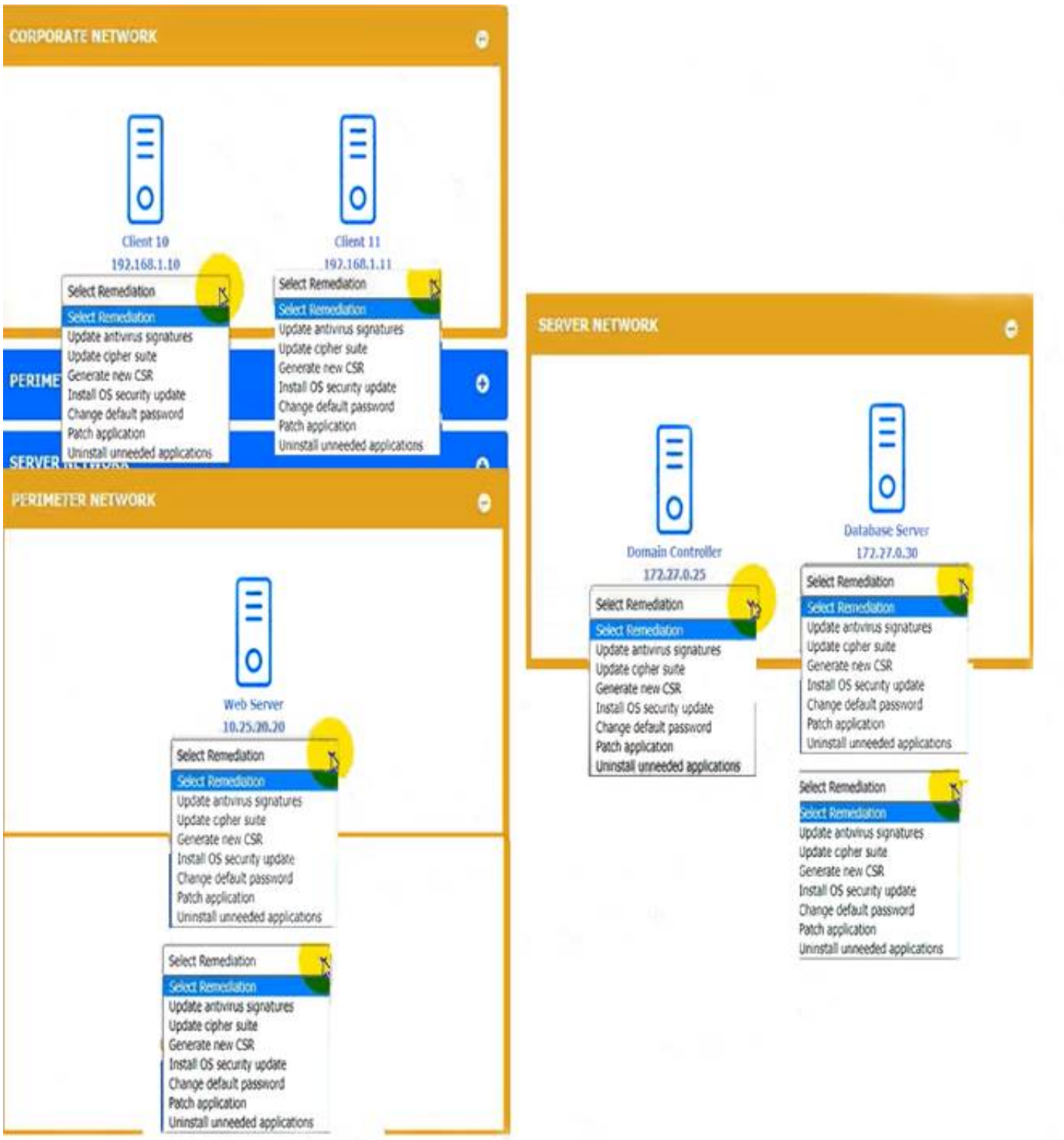
```
PORT     STATE
21/tcp   filtered
22/tcp   open
23/tcp   open
443/tcp  open
```

Which of the following should the analyst recommend to disable?

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

Answer: A

NEW QUESTION 106
- (Exam Topic 1)
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce. Remediation options may be selected multiple times, and some devices may require more than one
remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.

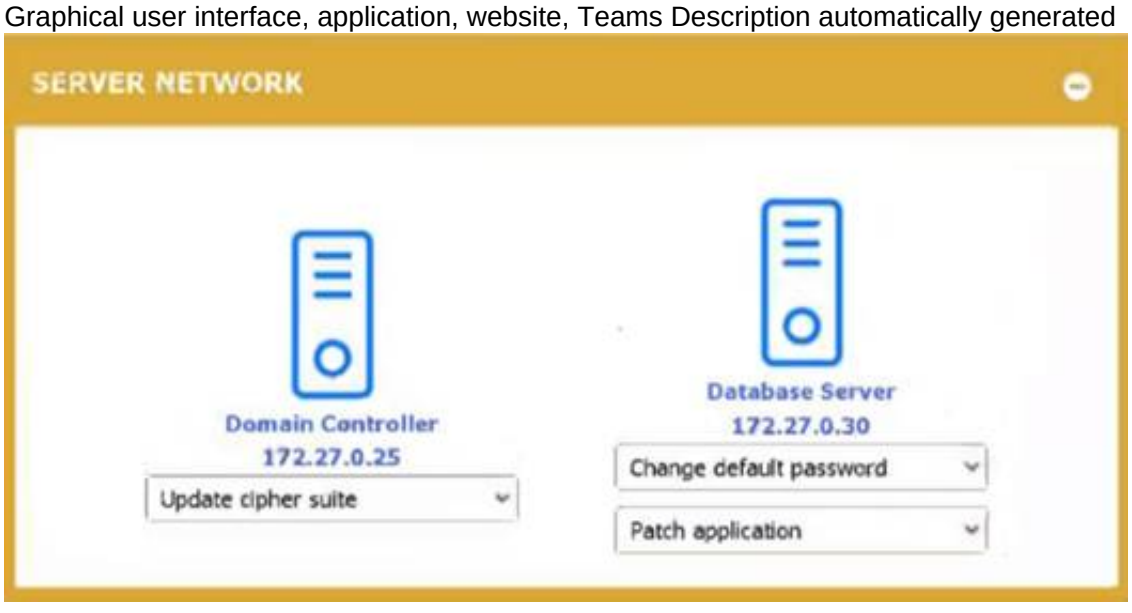


A. Mastered
B. Not Mastered

Answer: A

Explanation:

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



Graphical user interface, text, application Description automatically generated

NEW QUESTION 111
- (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 112
- (Exam Topic 1)
An employee's company account was used in a data breach Interviews with the employee revealed:
• The employee was able to avoid changing passwords by using a previous password again.
• The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.
Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)

A. Geographic dispersal
B. Password complexity
C. Password history
D. Geotagging
E. Password lockout
F. Geofencing

Answer: CF

Explanation:
two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofenc1in2g. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords1.
Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign region2s. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

NEW QUESTION 115
- (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 120
- (Exam Topic 1)
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

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

Answer: D

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

NEW QUESTION 123
- (Exam Topic 2)
Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

A. Firewall
B. SIEM
C. IPS
D. Protocol analyzer

Answer: B

Explanation:
SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes.
A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

NEW QUESTION 128
- (Exam Topic 2)
Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

A. Walk-throughs
B. Lessons learned
C. Attack framework alignment
D. Containment

Answer: B

Explanation:
After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as “lessons learned” and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

NEW QUESTION 129
- (Exam Topic 2)
Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

A. Access control
B. Syslog

C. Session Initiation Protocol traffic logs
D. Application logs

Answer: B

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

NEW QUESTION 131
- (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 132
- (Exam Topic 2)
A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the follow r 3 best describes these systems?

A. DNS sinkholes
B. Honey pots
C. Virtual machines
D. Neural networks

Answer: B

Explanation:
Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.

NEW QUESTION 133
- (Exam Topic 2)
Which of the following would satisfy three-factor authentication requirements?

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

Answer: C

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

NEW QUESTION 137
- (Exam Topic 2)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).

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

Answer: AC

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

NEW QUESTION 139
- (Exam Topic 2)
A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

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

Answer: C

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

NEW QUESTION 140
- (Exam Topic 2)
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?

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

Answer: A

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

NEW QUESTION 142
- (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 144
- (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 146
- (Exam Topic 2)
A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

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

Answer: BD

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

NEW QUESTION 147
- (Exam Topic 2)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Answer: AB

Explanation:
Geolocation and time-of-day restrictions would be best to mitigate the CEO’s concerns about staff members working from high-risk countries while on holiday or outsourcing work to a third-party organization in another country. Geolocation is a technique that involves determining the physical location of a device or user based on its IP address, GPS coordinates, Wi-Fi signals, or other indicators. Time-of-day restrictions are policies that limit the access or usage of resources based on the time of day or week. Geolocation and time-of-day restrictions can help to enforce access control rules, prevent unauthorized access, detect anomalous behavior, and comply with regulations. References: https://www.comptia.org/blog/what-is-geolocation
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 152
- (Exam Topic 2)
A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide

Answer: D

Explanation:
A secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies. A security analyst can create baselines for the server team to follow when hardening new devices for deployment based on a secure configuration guide.
* A. Change management procedure. This is not the correct answer, because a change management procedure is a document that describes the steps and processes for implementing, reviewing, and approving changes to an IT system or environment. A change management procedure helps to minimize the risks and impacts of changes on the system performance, availability, and security.
* B. Information security policy. This is not the correct answer, because an information security policy is a document that defines the rules and principles for protecting the confidentiality, integrity, and availability of information assets within an organization. An information security policy helps to establish the roles and responsibilities of employees, managers, and stakeholders regarding information security.
* C. Cybersecurity framework. This is not the correct answer, because a cybersecurity framework is a document that provides a set of standards, guidelines, and best practices for managing cybersecurity risks and improving resilience. A cybersecurity framework helps to align the business objectives and priorities with the security requirements and capabilities.
* D. Secure configuration guide. This is the correct answer, because a secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance

overall security by applying consistent and standardized settings and policies.
Reference: Secure Configuration Guide, Security Technical Implementation Guide - Wikipedia.

NEW QUESTION 155
- (Exam Topic 2)
An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

A. Base64 encoding
B. Steganography
C. Data encryption
D. Perfect forward secrecy

Answer: B

Explanation:
Steganography is a technique for hiding data inside of benign files such as images, audio, or video. This can be used to exfiltrate confidential data without raising suspicion or detection.
References: How to Hide Files Inside Files [Images, Folder] - Raymond.CC Blog; How to Hide Data in a Secret Text File Compartment - How-To Geek; How to Hide Data Within an Image - Medium

NEW QUESTION 156
- (Exam Topic 2)
An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian
B. Data controller
C. Data protection officer
D. Data processor

Answer: B

Explanation:
A data controller is an employee role that would determine the purpose of data and how to process it. A data controller is a person or entity that decides why and how personal data is collected, used, stored, shared, or deleted. A data controller has the responsibility to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and to ensure the rights and privacy of data subjects.
References: https://www.comptia.org/blog/what-is-a-data-controller
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 159
- (Exam Topic 2)
Server administrators want to configure a cloud solution so that computing memory and processor usage are maximized most efficiently across a number of virtual servers. They also need to avoid potential
denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation
B. High availability
C. Segmentation
D. Container security

Answer: A

Explanation:
Dynamic resource allocation is a technique that allows cloud providers to adjust the amount and distribution of computing resources according to the changing demand and capacity of the cloud environment1. Dynamic resource allocation can improve the efficiency and utilization of available computing power, as well as reduce the cost and energy consumption of the cloud infrastructure1. Dynamic resource allocation can also enhance the system availability and reliability by avoiding potential denial-of-service situations caused by overloading or under-provisioning of resources1.

NEW QUESTION 160
- (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 163
- (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 164
- (Exam Topic 2)
A security administrator examines the ARP table of an access switch and sees the following output:

VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

Which of the following is a potential threat that is occurring on this access switch?

A. DDoSonFa02 port
B. MAG flooding on Fa0/2 port
C. ARP poisoning on Fa0/1 port
D. DNS poisoning on port Fa0/1

Answer: C

Explanation:
ARP poisoning is a type of attack that exploits the ARP protocol to associate a malicious MAC address with a legitimate IP address on a network1. This allows the attacker to intercept, modify or drop traffic between the victim and other hosts on the same network. In this case, the ARP table of the access switch shows that the same MAC address (00-0c-29-58-35-3b) is associated with two different IP addresses (192.168.1.100 and 192.168.1.101) on port Fa0/12. This indicates that an attacker has poisoned the ARP table to redirect traffic intended for 192.168.1.100 to their own device with MAC address 00-0c-29-58-35-3b. The other options are not related to this scenario. DDoS is a type of attack that overwhelms a target with excessive traffic from multiple sources3. MAC flooding is a type of attack that floods a switch with fake MAC addresses to exhaust its MAC table and force it to operate as a hub4. DNS poisoning is a type of attack that corrupts the DNS cache with fake entries to redirect users to malicious websites.
References: 1: https://www.imperva.com/learn/application-security/arp-spoofing/ 2: https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148 3: https://www.imperva.com/learn/application-security/ddos-attack/ 4: https://www.imperva.com/learn/application-security/mac-flooding/ : https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/

NEW QUESTION 165
- (Exam Topic 2)
A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems. Which Of the following Company most likely complying with?

A. NIST CSF
B. GDPR
C. PCI OSS
D. ISO 27001

Answer: B

Explanation:
GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization’s systems under certain circumstances. This right is also known as the “right to be forgotten” or the “right to erasure”. An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://gdpr-info.eu/issues/right-to-be-forgotten/

NEW QUESTION 170
- (Exam Topic 2)
The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.
Which of the following would be the best way to safeguard this information without impeding the testing process?

A. Implementing a content filter
B. Anonymizing the data

C. Deploying DLP tools
D. Installing a FIM on the application server

Answer: B

Explanation:
Anonymizing the data is the process of removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous12. Anonymizing the data can safeguard the PHI records without impeding the testing process, because it can protect the privacy of the patients while preserving the data integrity and statistical accuracy for the application development team12. Anonymizing the data can be done by using techniques such as data masking, pseudonymization, generalization, data swapping, or data perturbation12.
Implementing a content filter is not the best way to safeguard the information, because it is a technique that blocks or allows access to certain types of content based on predefined rules or policies3. A content filter does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or leakage of PHI records.
Deploying DLP tools is not the best way to safeguard the information, because it is a technique that monitors and prevents data exfiltration or transfer to unauthorized destinations or users. DLP tools do not remove or encrypt PII from data sets, and they may not be sufficient to protect PHI records from internal misuse or negligence.
Installing a FIM on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of PHI records.

NEW QUESTION 172
- (Exam Topic 2)
A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

A. DDoS
B. Privilege escalation
C. DNS poisoning
D. Buffer overflow

Answer: A

Explanation:
A distributed denial-of-service (DDoS) attack is an attempt to make a computer or network resource unavailable to its intended users. This is accomplished by overwhelming the target with a flood of traffic from multiple sources.
In the scenario described, the security analyst identified a source IP address and blocked it from communicating with the network. However, the attack was still ongoing and coming from a large number of different source IP addresses. This indicates that the attack was a DDoS attack.
Privilege escalation is an attack that allows an attacker to gain unauthorized access to a system or network. DNS poisoning is an attack that modifies the DNS records for a domain name, causing users to be redirected to a malicious website. A buffer overflow is an attack that occurs when a program attempts to store more data in a buffer than it is designed to hold.
Therefore, the most likely type of attack in the scenario described is a DDoS attack.

NEW QUESTION 174
- (Exam Topic 2)
A company recently completed the transition from data centers to the cloud. Which of the following solutions will best enable the company to detect security threats in applications that run in isolated environments within the cloud environment?

A. Security groups
B. Container security
C. Virtual networks
D. Segmentation

Answer: B

Explanation:
Container security is a solution that can enable the company to detect security threats in applications that run in isolated environments within the cloud environment. Containers are units of software that package code and dependencies together, allowing applications to run quickly and reliably across different computing environments. Container security involves securing the container images, the container runtime, and the container orchestration platforms. Container security can help prevent unauthorized access, data breaches, malware infections, or denial-of-service attacks on the applications running in containers.
References: 1
CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3 : Summarize secure application development, deployment, and automation concepts 2
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 3
https://www.comptia.org/blog/what-is-container-security

NEW QUESTION 176
- (Exam Topic 2)
A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

A. IPSec
B. SFTP
C. SRTP
D. LDAPS
E. S/MIME
F. SSL VPN

Answer: AF

Explanation:
IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

NEW QUESTION 180
- (Exam Topic 2)
A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommended?

A. A content filter
B. AWAF
C. A next-generation firewall
D. An IDS

Answer: C

Explanation:
A next-generation firewall (NGFW) is a solution that can defend against malicious actors misusing protocols and being allowed through network defenses. A NGFW is a type of firewall that can perform deep packet inspection, application-level filtering, intrusion prevention, malware detection, and identity-based access control. A NGFW can also use threat intelligence and behavioral analysis to identify and block malicious traffic based on protocols, signatures, or anomalies.
References:
https://www.comptia.org/blog/what-is-a-next-generation-firewall
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 185
- (Exam Topic 2)
Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

A. Public cloud
B. Hybrid cloud
C. Community cloud
D. Private cloud

Answer: A

Explanation:
There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.
According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION 188
- (Exam Topic 2)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor

Answer: C

Explanation:
The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

NEW QUESTION 190
- (Exam Topic 2)
A security professional wants to enhance the protection of a critical environment that is Used to store and manage a company's encryption keys. The selected technology should be tamper resistant. Which of the following should the security professional implement to achieve the goal?

A. DLP
B. HSM
C. CA
D. FIM

Answer: B

Explanation:
HSM stands for hardware security module, which is a physical device that is used to store and manage cryptographic keys in a secure and tamper-resistant manner. HSMs can provide high-performance encryption and decryption operations, as well as key generation, backup, and recovery. HSMs can also prevent

unauthorized access or extraction of the keys, even by the cloud service provider or the HSM vendor. HSMs can enhance the protection of a critical environment that is used to store and manage encryption keys for a financial institution or any other organization that deals with sensitive data. References:

- https://www.comptia.org/certifications/security
- https://www.professormesser.com/security-plus/sy0-501/hardware-security-3/

NEW QUESTION 195
- (Exam Topic 2)
A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

A. Shoulder surfing
B. Watering hole
C. Vishing
D. Tailgating

Answer: A

Explanation:
Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to see what they are typing, writing, or viewing on their screen. It can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer's credit card number during a phone call.

NEW QUESTION 198
- (Exam Topic 2)
A network engineer is troubleshooting wireless network connectivity issues that were reported by users The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building There have also been reports of users being required to enter their credentials on web pages in order to gain access to them Which of the following is the most likely cause of this issue?

A. An external access point is engaging in an evil-Twin attack
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled
D. The users in that section of the building are on a VLAN that is being blocked by the firewall

Answer: A

Explanation:
An evil-Twin attack is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. It is the most likely cause of the issue that users are experiencing slow speeds, unable to connect to network drives, and required to enter their credentials on web pages when working in the section of the building that is closest to the parking lot, where an external access point could be placed nearby.

NEW QUESTION 200
- (Exam Topic 2)
An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's need?

A. MFA
B. 802.1X
C. WPA2
D. TACACS

Answer: B

Explanation:
* 802.1 X is a standard for network access control that provides authentication and encryption for devices that connect to a LAN/WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (the device requesting access), an authenticator (the device granting access), and an authentication server (the device verifying credentials). 802.1X can prevent on-path attacks and evil twin attacks by requiring users to provide valid credentials before accessing the network and encrypting the data transmitted over the network.
On-path attacks are attacks that involve intercepting or modifying network traffic between two endpoints. An on-path attacker can eavesdrop on sensitive information, alter or inject malicious data, or redirect traffic to malicious destinations. On-path attacks are frequently perpetrated over WiFi network1s.
Evil twin attacks are attacks that involve setting up a fake WiFi access point that mimics a legitimate one. An evil twin attacker can trick users into connecting to the fake network and then monitor or manipulate their online activity. Evil twin attacks are more common on public WiFi networks that are unsecured and leave personal data vulnerable23.

NEW QUESTION 204
- (Exam Topic 2)
A network administrator has been alerted that web pages are experiencing long load times After determining it is not a routing or DNS issue the administrator logs in to the router, runs a command, and receives the following output:
CPU 0 percent busy, from 300 sec ago 1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
Which of the following is The router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

Answer: D

Explanation:
The router is experiencing a resource exhaustion issue. The output from the command indicates that the CPU is consistently busy, with a 1-second average of 99 percent busy and a 1-minute average of 83 percent busy.
This indicates that the router is struggling to keep up with the demands placed on it, potentially due to a high volume of traffic or other factors. As a result, web pages are experiencing long load times. This is an example of resource exhaustion, where the router's resources are being overwhelmed and are unable to meet the demands placed on them. A DDoS attack, memory leak, or buffer overflow would not typically cause the symptoms described in the scenario.

NEW QUESTION 208
- (Exam Topic 2)
A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?

A. Measured boot
B. Boot attestation
C. UEFI
D. EDR

Answer: B

Explanation:
Boot attestation is a security feature that enables the computer to verify the integrity of its operating system
before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.
According to the CompTIA Security+ Study Guide, “Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time.”

NEW QUESTION 213
- (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 217
- (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 220
- (Exam Topic 2)
A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company’s mobile application. After reviewing the back-end

server logs, the security analyst finds the following entries:

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/client_id=1 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/client_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/client_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/client_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:18 +0100] "GET /api/client_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

Which of the following is the most likely cause of the security control bypass?

A. IP address allow list
B. User-agent spoofing
C. WAF bypass
D. Referrer manipulation

Answer: B

Explanation:
User-agent spoofing is a technique that involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

NEW QUESTION 223
- (Exam Topic 2)
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

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

Answer: A

Explanation:
SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine1. SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

NEW QUESTION 225
- (Exam Topic 2)
A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

A. SIEM
B. HIDS
C. CASB
D. EDR

Answer: A

Explanation:
SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

NEW QUESTION 226
- (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 230

- (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 233
- (Exam Topic 2)
A security analyst needs to implement security features across smartphones. laptops, and tablets. Which of the following would be the most effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

Answer: D

Explanation:
MDM stands for Mobile Device Management, which is a software solution that can manage and secure smartphones, laptops, tablets and other mobile devices across heterogeneous platforms. MDM can enforce security features such as encryption, password policies, remote wipe, device tracking, app control and more. MDM can also monitor and update the devices remotely and provide reports and alerts on their status. MDM is the most effective solution to implement security features across heterogeneous platforms, as it can provide centralized and consistent management of various types of devices. Verified References:
- Security+ (Plus) Certification | CompTIA IT Certifications
https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.4: Given a scenario, implement secure systems design.)
- CompTIA Security+ 601 - Infosec
https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf (See Security+: 5 in-demand cybersecurity skills, Implementation)
- Certification Security+ | CompTIA https://www.comptia.org/landing/securityplus/index.html (See Exam Objectives)

NEW QUESTION 238
- (Exam Topic 2)
After installing a patch On a security appliance. an organization realized a massive data exfiltration occurred. Which Of the following describes the incident?

A. Supply chain attack
B. Ransomware attack
C. Cryptographic attack
D. Password attack

Answer: A

Explanation:
A supply chain attack is a type of attack that involves compromising a trusted third-party provider or vendor and using their products or services to deliver malware or gain access to the target organization. The attacker can exploit the trust and dependency that the organization has on the provider or vendor and bypass their security controls. In this case, the attacker may have tampered with the patch for the security appliance and used it to exfiltrate data from the organization.

NEW QUESTION 243
- (Exam Topic 2)
A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select two).

A. Chain of custody
B. Tags
C. Reports
D. Time stamps
E. Hash values
F. Time offset

Answer: DF

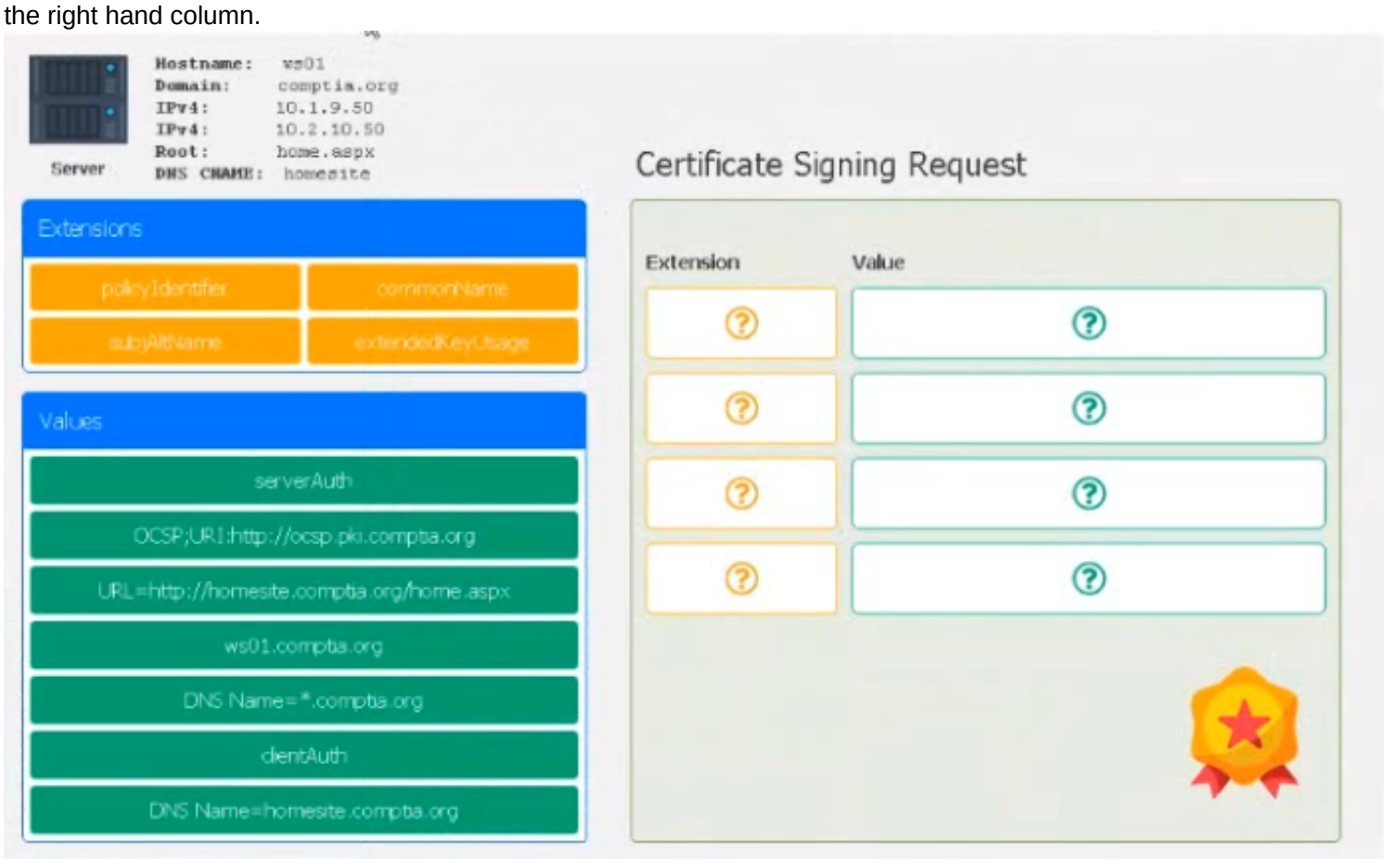
Explanation:
A server farm’s logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.
To determine the sequence of a server farm’s logs, the administrator should consider the following factors:
- Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across

different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

- Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

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-server/administration/server-manager/view-event-logs

NEW QUESTION 244
- (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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 245
- (Exam Topic 2)
The new Chief Information Security Officer at a company has asked the security learn to implement stronger user account policies. The new policies require:
• Users to choose a password unique to their last ten passwords
• Users to not log in from certain high-risk countries
Which of the following should the security team implement? (Select two).

A. Password complexity
B. Password history
C. Geolocation
D. Geospatial
E. Geotagging
F. Password reuse

Answer: BC

Explanation:
Password history is a policy that prevents users from reusing their previous passwords. This can reduce the risk of password cracking or compromise. Geolocation is a policy that restricts users from logging in from certain locations based on their IP address. This can prevent unauthorized access from high-risk countries or regions. References: https://www.comptia.org/content/guides/what-is-identity-and-access-management

NEW QUESTION 247
- (Exam Topic 2)
Which Of the following will provide the best physical security countermeasures to Stop intruders? (Select two).

A. Alarm
B. Signage
C. Lighting
D. Access control vestibules
E. Fencing
F. Sensors

Answer: CE

Explanation:
Lighting and fencing are physical security countermeasures that can deter or stop intruders from accessing a facility or an asset. Lighting can increase visibility and reduce hiding spots for intruders, while fencing can create a physical barrier and limit access points for intruders.

NEW QUESTION 250
- (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 251
- (Exam Topic 2)
A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

A. Cameras
B. Badges
C. Locks
D. Bollards

Answer: B

Explanation:
Badges are physical security controls that provide a way to identify and authenticate authorized individuals
who need to access a building or a restricted area. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.

NEW QUESTION 255
- (Exam Topic 2)
A security analyst receives an alert from the company's S1EM that anomalous activity is coming from a local source IP address of 192 168 34.26 The Chief Information Security Officer asks the analyst to block the originating source Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed property. The IP address the employee provides is 192 168.34 26. Which of the following describes this type of alert?

A. True positive
B. True negative
C. False positive
D. False negative

Answer: C

Explanation:
A false positive is a type of alert that indicates a security incident when there is none. It can be caused by misconfigured or overly sensitive security tools or systems that generate false or irrelevant alerts. In this case, the alert from the company’s SIEM that Mimikatz attempted to run on the remote systems was a false positive because it was triggered by a legitimate vulnerability scanning tool that uses Mimikatz as part of its functionality.

NEW QUESTION 259
- (Exam Topic 2)
A large bank with two geographically dispersed data centers Is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages thai last (or a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator

C. PDU
D. Dally backups

Answer: B

Explanation:
A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

NEW QUESTION 264
- (Exam Topic 2)
While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements. Which of the following would be the BEST solution to securely prevent future issues?

A. Using an administrator account to run the processes and disabling the account when it is not in use
B. Implementing a shared account the team can use to run automated processes
C. Configuring a service account to run the processes
D. Removing the password complexity requirements for the user account

Answer: C

Explanation:
A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 268
- (Exam Topic 2)
During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall. Which of the following describes the
greatest risk associated with using FTP?

A. Private data can be leaked
B. FTP is prohibited by internal policy.
C. Users can upload personal files
D. Credentials are sent in cleartex

Answer: D

Explanation:
Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk. Users can upload personal files (Option C) is a management issue, but not a security risk
https://www.infosectrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/

NEW QUESTION 269
- (Exam Topic 2)
During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production Which of the following describes what the company should do first to lower the risk to the
Production the hardware.

A. Back up the hardware.
B. Apply patches.
C. Install an antivirus solution.
D. Add a banner page to the hardware.

Answer: B

Explanation:
Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. References: 1
CompTIA Security+
Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize
secure application development, deployment, and automation concepts 2
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 3 https://www.comptia.org/blog/patch-management-best-practices

NEW QUESTION 270
- (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 275
- (Exam Topic 2)
A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?

A. Recovery
B. Lessons learned
C. Containment
D. Preparation

Answer: C

Explanation:
Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact. Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration
https://www.fortinet.com/resources/cyberglossary/incident-response https://www.ibm.com/topics/incident-response

NEW QUESTION 279
- (Exam Topic 2)
A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is most likely preventing the IT manager at the hospital from upgrading the specialized OS?

A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.
B. The MRI vendor does not support newer versions of the OS.
C. Changing the OS breaches a support SLA with the MRI vendor.
D. The IT team does not have the budget required to upgrade the MRI scanner.

Answer: B

Explanation:
This option is the most likely reason for preventing the IT manager at the hospital from upgrading the specialized OS. The MRI scanner is a complex and sensitive device that requires a specific OS to control and operate it. The MRI vendor may not have developed or tested newer versions of the OS for compatibility and functionality with the scanner. Upgrading the OS without the vendor’s support may cause the scanner to malfunction or stop working altogether.

NEW QUESTION 282
- (Exam Topic 2)
An organization decided not to put controls in place because of the high cost of implementing the controls
compared to the cost of a potential fine. Which of the following risk management strategies is the organization following?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

Answer: D

Explanation:
Acceptance is a risk management strategy that involves acknowledging the existence and potential impact of a risk, but deciding not to take any action to reduce or eliminate it. This strategy is usually adopted when the cost of implementing controls outweighs the benefit of mitigating the risk, or when the risk is deemed acceptable or unavoidable. In this case, the organization decided not to put controls in place because of the high cost compared to the potential fine, which means they accepted the risk. References: https://www.comptia.org/blog/what-is-risk-acceptance

NEW QUESTION 283
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

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

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

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