Exam Questions SY0-701

CompTIA Security+ Exam

https://www.2passeasy.com/dumps/SY0-701/

NEW QUESTION 1
Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

A. Encrypted
B. Intellectual property
C. Critical
D. Data in transit

Answer: B

Explanation:
Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market. Therefore, these employees receive extensive training to ensure
they understand how to best protect this type of data. References = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

NEW QUESTION 2
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

Answer: B

Explanation:
= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances – SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

NEW QUESTION 3
A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO
B. LEAP
C. MFA
D. PEAP

Answer: A

Explanation:
SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
* B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4.
* C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
* D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.
References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

NEW QUESTION 4
Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems
D. SCADA

Answer: B

Explanation:
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

NEW QUESTION 5
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Answer: D

Explanation:
A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:
Access list <direction> <action> <source address> <destination address> <protocol>
<port>
To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4, page 175.

NEW QUESTION 6
Which of the following allows for the attribution of messages to individuals?

A. Adaptive identity
B. Non-repudiation
C. Authentication
D. Access logs

Answer: B

Explanation:
Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it.
Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document. References = Non- repudiation – CompTIA Security+ SY0-701 – 1.2, CompTIA Security+ SY0-301: 6.1 – Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

NEW QUESTION 7
A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

A. MSA
B. SLA
C. BPA
D. SOW

Answer: D

Explanation:
An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome. For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training.
The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations
of the partnership. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: Contracts and Agreements (5:12).

NEW QUESTION 8
Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape
B. SQL injection

C. Buffer overflow
D. Race condition

Answer: C

Explanation:
A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

NEW QUESTION 9
Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement
B. Supply chain analysis
C. Right to audit clause
D. Due diligence

Answer: A

Explanation:
 Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:
? The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
? The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
? The testing team credentials and the authorized tools and techniques that they can use.
? The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
? The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
? The timeline and duration of the test, and the hours of operation and testing windows.
? The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.
Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.
References = https://www.yeahhub.com/every-penetration-tester-you-should-know-about- this-rules-of-engagement/
https://bing.com/search?q=rules+of+engagement+penetration+testing

NEW QUESTION 10
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction

Answer: D

Explanation:
 The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.
One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.
The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.
References = https://bing.com/search?q=Zero+Trust+data+plane https://learn.microsoft.com/en-us/security/zero-trust/deploy/data

NEW QUESTION 10
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication
B. Permissions assignment
C. Access management
D. Password complexity

Answer: A

Explanation:
The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management © is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References = You can learn more about multifactor authentication and other security concepts in the following resources:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1
? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2
? Multi-factor Authentication – SY0-601 CompTIA Security+ : 2.43
? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4
? CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

NEW QUESTION 11
An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

Answer: D

Explanation:
Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.
References:
? Official CompTIA Security+ Study Guide (SY0-701), page 29
? Security Controls - CompTIA Security+ SY0-701 - 1.1 1

NEW QUESTION 14
Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

A. SIEM
B. DLP
C. IDS
D. SNMP

Answer: A

Explanation:
SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

NEW QUESTION 18
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A. Private
B. Critical
C. Sensitive
D. Public

Answer: C

Explanation:
Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.
Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.
Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.
Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.
Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.
Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

NEW QUESTION 20
A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

Answer: C

Explanation:
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

NEW QUESTION 21
Which of the following must be considered when designing a high-availability network? (Select two).

A. Ease of recovery
B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

Answer: AE

Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.
Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation. Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4:
Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0- 701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

NEW QUESTION 23
A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off\
B. http://
C. www.*.com
D. :443

Answer: B

Explanation:
A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling", "porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.
To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.
The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext

transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol.

:443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION 27
Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select two).

A. Channels by which the organization communicates with customers
B. The reporting mechanisms for ethics violations
C. Threat vectors based on the industry in which the organization operates
D. Secure software development training for all personnel
E. Cadence and duration of training events
F. Retraining requirements for individuals who fail phishing simulations

Answer: CE

Explanation:
A training curriculum plan for a security awareness program should address the following factors:
? The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking1.
? The cadence and duration of training events. This will help the employees to retain
the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

NEW QUESTION 30
A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance
B. Patching
C. Segmentation
D. Replacement

Answer: C

Explanation:
Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

NEW QUESTION 31
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?

A. Scalability
B. Availability
C. Cost
D. Ease of deployment

Answer: B

Explanation:
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of- service attacks, and have backup and recovery plans in case of failures2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

NEW QUESTION 36
An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting
B. Phishing
C. Impersonation
D. Vishing
E. Smishing
F. Misinformation

Answer: BE

Explanation:

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action12. In this scenario, the text message that claims to be from the payroll department is an example of smishing.

Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-person visits, and can be used to obtain information, access, or money from the victim34. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

* A. Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads56. Typosquatting is not related to text messages or credential verification.

* B. Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action78. Phishing is not related to text messages or credential verification.

* D. Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply9 . Vishing is not related to text messages or credential verification.

* F. Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda . Misinformation is not related to text messages or credential verification.

References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3: Impersonation Attacks: What Are They and How Do You Protect Against

Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

NEW QUESTION 38
After a security incident, a systems administrator asks the company to buy a NAC platform. Which of the following attack surfaces is the systems administrator trying to protect?

A. Bluetooth
B. Wired
C. NFC
D. SCADA

Answer: B

Explanation:

A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network12.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5, page 189; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 237.

NEW QUESTION 39
Which of the following would be the best way to block unknown programs from executing?

A. Access control list
B. Application allow list.
C. Host-based firewall
D. DLP solution

Answer: B

Explanation:

An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network12.

The other options are not the best ways to block unknown programs from executing:

? Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing13.

? Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing1 .

? DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing1 .

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting – CompTIA Security+ SY0-701 – 3.5, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

NEW QUESTION 41
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

Answer: D

Explanation:
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION 43
Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP
B. CSR
C. CA
D. CRC

Answer: A

Explanation:
OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

NEW QUESTION 44
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?

A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests

Answer: B

Explanation:
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

NEW QUESTION 46
The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

Answer: A

Explanation:
Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance1.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 35.

NEW QUESTION 49
After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

A. Group Policy
B. Content filtering
C. Data loss prevention
D. Access control lists

Answer: D

Explanation:
Access control lists (ACLs) are rules that specify which users or groups can access which resources on a file server. They can help restrict access to confidential data by granting or denying permissions based on the identity or role of the user. In this case, the administrator can use ACLs to quickly modify the access rights of the users and prevent them from accessing the data they are not authorized to
see. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

NEW QUESTION 50
A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

A. Processor
B. Custodian
C. Subject
D. Owner

Answer: C

Explanation:
According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.
ReferencesCompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

NEW QUESTION 55
A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

A. Set the maximum data retention policy.
B. Securely store the documents on an air-gapped network.
C. Review the documents' data classification policy.
D. Conduct a tabletop exercise with the team.

Answer: D

Explanation:
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

NEW QUESTION 59
An organization recently updated its security policy to include the following statement:
Regular expressions are included in source code to remove special characters such as $, |, ;. &, `, and ? from variables set by forms in a web application.
Which of the following best explains the security technique the organization adopted by making this addition to the policy?

A. Identify embedded keys
B. Code debugging
C. Input validation
D. Static code analysis

Answer: C

Explanation:
Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as $, |, ;, &, `, and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.
Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.
References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security – SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

NEW QUESTION 63
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53
D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53

Answer: D

Explanation:
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other

devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B). References = You can learn more about firewall ACLs and DNS in the following resources:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

NEW QUESTION 68
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

Answer: C

Explanation:
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats. One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:
? Applying patches and updates to the operating system and the application, if available
? Removing or disabling unnecessary services, features, or accounts
? Configuring firewall rules and network access control lists to restrict inbound and outbound traffic
? Enabling encryption and authentication for data transmission and storage
? Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity
? Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible. References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

NEW QUESTION 72
A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

A. Secure cookies
B. Version control
C. Input validation
D. Code signing

Answer: C

Explanation:
Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users. Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security – SY0-601 CompTIA Security+ : 3.2

NEW QUESTION 77
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

Answer: AC

Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

NEW QUESTION 81

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC
B. ACL
C. SAML
D. GPO

Answer: A

Explanation:
RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

NEW QUESTION 83
Which of the following is the most likely to be included as an element of communication in a security awareness program?

A. Reporting phishing attempts or other suspicious activities
B. Detecting insider threats using anomalous behavior recognition
C. Verifying information when modifying wire transfer data
D. Performing social engineering as part of third-party penetration testing

Answer: A

Explanation:
A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.
The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training –
CompTIA Security+ SY0-701: 5.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

NEW QUESTION 87
Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

A. Automation
B. Compliance checklist
C. Attestation
D. Manual audit

Answer: A

Explanation:
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.
The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:
? Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.
? Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.
? Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION 88
Which of the following describes the reason root cause analysis should be conducted as part of incident response?

A. To gather loCs for the investigation
B. To discover which systems have been affected
C. To eradicate any trace of malware on the network
D. To prevent future incidents of the same nature

Answer: D

Explanation:
Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather loCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment
and eradication phases of incident response. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

NEW QUESTION 90
Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation

Answer: C

Explanation:
Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non- repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

NEW QUESTION 95
Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."
Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

Answer: BC

Explanation:
This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money.
References = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

NEW QUESTION 96
Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist

Answer: C

Explanation:
A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare12. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542:

Threat Actors – CompTIA
Security+ SY0-701 – 2.1, video by Professor Messer.

NEW QUESTION 100
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation
B. Isolation
C. Patching
D. Encryption

Answer: A

Explanation:
 Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION 104
After reviewing the following vulnerability scanning report:
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
A security analyst performs the following test: nmap -p 23 192.168.14.6 —script telnet-encryption PORT STATE SERVICE REASON
23/tcp open telnet syn-ack I telnet encryption:
| _ Telnet server supports encryption
Which of the following would the security analyst conclude for this reported vulnerability?

A. It is a false positive.
B. A rescan is required.
C. It is considered noise.
D. Compensating controls exist.

Answer: A

Explanation:
A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly3. References: 3: Telnet Protocol - Can You Encrypt Telnet?

NEW QUESTION 109
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

A. Virus
B. Trojan
C. Spyware
D. Ransomware

Answer: D

Explanation:
 Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

NEW QUESTION 110
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active
B. Passive
C. Defensive
D. Offensive

Answer: A

Explanation:
 Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they

involve probing the target for specific information. References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

NEW QUESTION 114
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-701 Product From:

https://www.2passeasy.com/dumps/SY0-701/

Money Back Guarantee

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

* SY0-701 Practice Questions Verified by Expert Senior Certified Staff

* SY0-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year