CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

NEW QUESTION 1
- (Exam Topic 1)
A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

A. Identity theft
B. RFID cloning
C. Shoulder surfing
D. Card skimming

Answer: D

Explanation:
The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 5

NEW QUESTION 2
- (Exam Topic 1)
A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backup followed by different backups

Answer: B

Explanation:
The best backup strategy for minimizing the number of backups that need to be restored in case of data loss is full backups followed by incremental backups. This strategy allows for a complete restoration of data by restoring the most recent full backup followed by the most recent incremental backup. Reference: CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) page 126

NEW QUESTION 3
- (Exam Topic 1)
A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

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

Answer: A

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

NEW QUESTION 4
- (Exam Topic 1)
A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system Which of the following would be BEST suited for this task?

A. Social media analysis
B. Annual information security training
C. Gamification
D. Phishing campaign

Answer: D

Explanation:
A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

NEW QUESTION 5
- (Exam Topic 1)
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. laC
B. MSSP

C. Containers
D. SaaS

Answer: A

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

NEW QUESTION 6
- (Exam Topic 1)
A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

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

Answer: D

Explanation:
If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:
CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

NEW QUESTION 7
- (Exam Topic 1)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

Answer: A

Explanation:
PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data1. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet1.
One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for2. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org2. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org2.
Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used3. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years3. The validity period can be checked by looking at the valid from and valid to dates on the certificate3.
Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org2. It also has a validity period of one year, which means it needs to be rotated annually3.

NEW QUESTION 8
- (Exam Topic 1)
A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.
B. Define the PC firewall rules to limit access.
C. Encrypt the disk on the storage device.
D. Plug the storage device in to the UPS

Answer: A

Explanation:
The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

NEW QUESTION 9
- (Exam Topic 1)
A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 1)
A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?

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

Answer: B

Explanation:
Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems. References: CompTIA Security+ Study Guide 601, Chapter 4

NEW QUESTION 10
- (Exam Topic 1)
Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

A. White team
B. Purple team
C. Green team
D. Blue team
E. Red team

Answer: A

Explanation:
During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively. They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures.

NEW QUESTION 12
- (Exam Topic 1)
A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update
B. HTTP headers
C. Secure cookies
D. Third-party updates
E. Full disk encryption
F. Sandboxing
G. Hardware encryption

Answer: AF

Explanation:
Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.
Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary. Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

NEW QUESTION 13
- (Exam Topic 1)
Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

Answer: A

Explanation:
A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

NEW QUESTION 14

- (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 15
- (Exam Topic 1)
When planning to build a virtual environment, an administrator need to achieve the following,
•Establish polices in Limit who can create new VMs
•Allocate resources according to actual utilization‘
•Require justication for requests outside of the standard requirements.
•Create standardized categories based on size and resource requirements Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication
B. Product against VM escape
C. Deploy a PaaS
D. Avoid VM sprawl

Answer: D

Explanation:
The administrator is most likely trying to avoid VM sprawl, which occurs when too many VMs are created and managed poorly, leading to resource waste and increased security risks. The listed actions can help establish policies, resource allocation, and categorization to prevent unnecessary VM creation and ensure proper management. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.6 Given a scenario, implement the appropriate virtualization components.

NEW QUESTION 18
- (Exam Topic 1)
An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?

A. TPM
B. CA
C. SAML
D. CRL

Answer: A

Explanation:
The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

NEW QUESTION 20
- (Exam Topic 1)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user’s PCs. Which of the following is the most likely cause of this issue?

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

Answer: B

Explanation:
SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device12. SSH can encrypt both the authentication information and the data being exchanged between the client and the server2. SSH can be used to access and manage a NAS device remotely3.

NEW QUESTION 25
- (Exam Topic 1)
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT

B. Ransomware
C. Polymophic
D. A worm

Answer: A

Explanation:
Based on the given information, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan). RATs are often used for stealthy unauthorized access to a victim's computer, and they can evade traditional antivirus software through various sophisticated techniques. In particular, the fact that the malware is communicating with external IP addresses during specific hours suggests that it may be under the control of an attacker who is issuing commands from a remote location. Ransomware, polymorphic malware, and worms are also possible culprits, but the context of the question suggests that a RAT is the most likely answer.

NEW QUESTION 26
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

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

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-phishing

NEW QUESTION 27
- (Exam Topic 1)
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable
To improve security? (Select TWO.)

A. RADIUS
B. PEAP
C. WPS
D. WEP-EKIP
E. SSL
F. WPA2-PSK

Answer: AF

Explanation:
To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

NEW QUESTION 29
- (Exam Topic 1)
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
• All users share workstations throughout the day.
• Endpoint protection was disabled on several workstations throughout the network.
• Travel times on logins from the affected users are impossible.
• Sensitive data is being uploaded to external sites.
• All user account passwords were forced to be reset and the issue continued. Which of the following attacks is being used to compromise the user accounts?

A. Brute-force
B. Keylogger
C. Dictionary
D. Rainbow

Answer: B

Explanation:
The symptoms suggest a keylogger is being used to compromise the user accounts, allowing the attackers to obtain the users' passwords and other sensitive information. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 30

- (Exam Topic 1)
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

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

Answer: C

Explanation:
Detailed
Password spraying is an attack where an attacker tries a small number of commonly used passwords against a large number of usernames. The goal of password spraying is to avoid detection by avoiding too many failed login attempts for any one user account. The fact that different usernames are being attacked from the same IP address is a strong indication that a password spraying attack is underway.

NEW QUESTION 31
- (Exam Topic 1)
A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

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

Answer: A

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

NEW QUESTION 34
- (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 36
- (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 41
- (Exam Topic 1)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: DE

Explanation:
The most likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases are included third-party libraries and vendors/supply chain. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Supply Chain and Software Development Life Cycle

NEW QUESTION 44
- (Exam Topic 1)
During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s
B. chflags
C. chmod
D. lsof
E. setuid

Answer: C

Explanation:
The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 45
- (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 50
- (Exam Topic 1)
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules,
C. Emulate the malware in a heavily monitored DMZ segment
D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:
Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques. References: CompTIA Security+ Study Guide, page 129

NEW QUESTION 54
- (Exam Topic 1)
Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

A. RTO

B. MTBF
C. MTTR
D. RPO

Answer: C

Explanation:
Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment. References: CompTIA Security+ Certification Exam Objectives 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.

NEW QUESTION 55
- (Exam Topic 1)
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

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

Answer: C

Explanation:
Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 1: Attacks, Threats, and Vulnerabilities

NEW QUESTION 59
- (Exam Topic 1)
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

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

Answer: C

Explanation:
One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

NEW QUESTION 64
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling
B. Spam
C. Invoice scam
D. Pharming

Answer: A

Explanation:
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

NEW QUESTION 65
- (Exam Topic 1)
An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP
B. SAML
C. SSO
D. Kerberos

Answer: C

Explanation:
Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials. References: CompTIA Security+ Study Guide 601, Chapter 6

NEW QUESTION 69
- (Exam Topic 1)
A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

•Must be able to differentiate between users connected to WiFi
•The encryption keys need to change routinely without interrupting the users or forcing reauthentication
•Must be able to integrate with RADIUS
•Must not have any open SSIDs
Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise
B. WPA3-PSK
C. 802.11n
D. WPS

Answer: A

Explanation:
Detailed
WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication. Additionally, WPA2-Enterprise does not allow for open SSIDs.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7: Securing Networks, p. 317

NEW QUESTION 72
- (Exam Topic 1)
A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

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

Answer: C

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

NEW QUESTION 74
- (Exam Topic 1)
A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral

Answer: CD

Explanation:
An identity provider (IdP) is responsible for authenticating users and generating security tokens containing user information. A service provider (SP) is responsible for accepting security tokens and granting access to resources based on the user's identity.

NEW QUESTION 78
- (Exam Topic 1)
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates

Answer: C

Explanation:
When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network. This prevents the malware from spreading and potentially infecting other hosts. Adding a
deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. References: CompTIA Security+ Study Guide, pages 113-114

NEW QUESTION 83
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands

on the gateway and obtains the following output:

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

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

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

Answer: C

Explanation:
The output of the “netstat -ano” command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.
The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client’s browser.
Based on the output of the “netstat -ano” command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.
ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION 85
- (Exam Topic 1)
Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

A. TOTP
B. Biometrics
C. Kerberos
D. LDAP

Answer: A

Explanation:
Time-based One-Time Password (TOTP) is a type of authentication method that sends out a unique password to be used within a specific number of seconds. It uses a combination of a shared secret key and the current time to generate a one-time password. TOTP is commonly used for two-factor authentication (2FA) to provide an additional layer of security beyond just a username and password.

NEW QUESTION 89
- (Exam Topic 1)
An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware
B. Hash substitution
C. Collision
D. Phishing

Answer: B

Explanation:
This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

NEW QUESTION 93
- (Exam Topic 1)
The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?

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

Answer: A

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

NEW QUESTION 94
- (Exam Topic 1)
A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover

which vulnerable services are running?

A. Non-credentialed
B. Web application
C. Privileged
D. Internal

Answer: C

Explanation:
Privileged scanning, also known as credentialed scanning, is a type of vulnerability scanning that uses a valid user account to log in to the target host and examine vulnerabilities from a trusted user's perspective. It can provide more accurate and comprehensive results than unprivileged scanning, which does not use any credentials and only scans for externally visible vulnerabilities.

NEW QUESTION 99
- (Exam Topic 1)
An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

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

Answer: C

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

NEW QUESTION 103
- (Exam Topic 2)
A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

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

Answer: D

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

NEW QUESTION 104
- (Exam Topic 2)
The application development teams have been asked to answer the following questions:
- Does this application receive patches from an external source?
- Does this application contain open-source code?
- Is this application accessible by external users?
- Does this application meet the corporate password standard? Which of the following are these questions part of?

A. Risk control self-assessment
B. Risk management strategy
C. Risk acceptance
D. Risk matrix

Answer: A

Explanation:
A risk control self-assessment (RCSA) is a process that allows an organization to identify, evaluate, and mitigate the risks associated with its activities, processes, systems, and products. A RCSA involves asking relevant questions to assess the effectiveness of existing controls and identify any gaps or weaknesses that need improvement. A RCSA also helps to align the risk appetite and tolerance of the organization with its strategic objectives and performance.
The application development teams have been asked to answer questions related to their applications' security posture, such as whether they receive patches from an external source, contain open-source code, are accessible by external users, or meet the corporate password standard. These questions are part of a RCSA process that aims to evaluate the potential risks and vulnerabilities associated with each application and determine how well they are managed and mitigated.

NEW QUESTION 109
- (Exam Topic 2)
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting

B. Buffer overflow
C. Jailbreaking
D. Side loading

Answer: C

Explanation:
Jailbreaking is the vulnerability that the organization is addressing by adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Jailbreaking is the process of removing the restrictions or limitations imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking can allow users to install unauthorized applications, customize settings, or access system files. However, jailbreaking can also expose the device to security risks, such as malware, data loss, or warranty voidance. References: https://www.comptia.org/blog/what-is-jailbreaking https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 111
- (Exam Topic 2)
A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race Which of the following best describes this type of information?

A. Sensitive
B. Non-Pll
C. Private
D. Confidential

Answer: B

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

NEW QUESTION 113
- (Exam Topic 2)
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 follow r 3 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 114
- (Exam Topic 2)
Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?

A. Vendor management
B. Application programming interface
C. Vanishing
D. Encryption strength
E. Firmware

Answer: E

Explanation:
Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks1. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices1, or you can use a network monitoring software to keep track of the firmware status of your devices2. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION 118
- (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 m a secure manner?

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

Answer: B

Explanation:
Key exchange Short
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

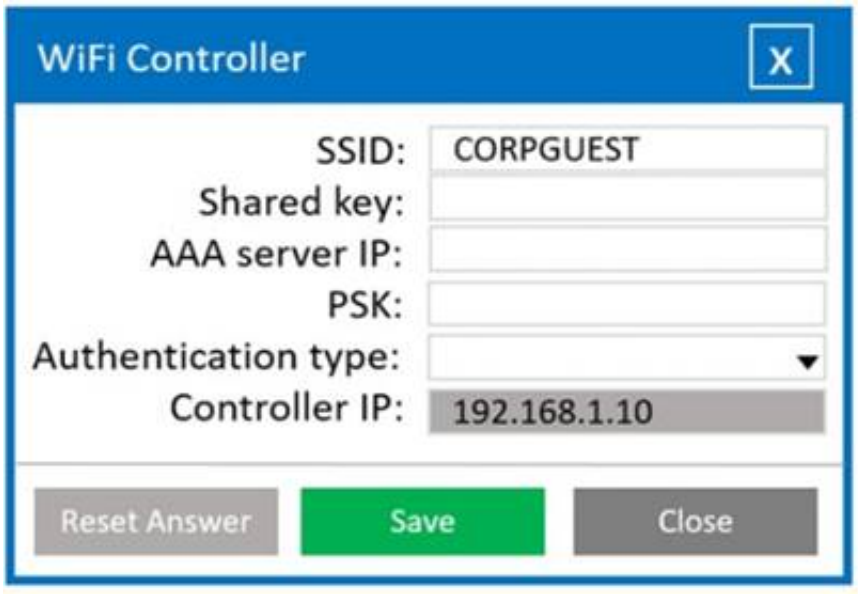
NEW QUESTION 123
- (Exam Topic 2)
A security analyst receives an alert that indicates a user's device is displaying anomalous behavior The analyst suspects the device might be compromised Which of the following should the analyst to first?

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 126
- (Exam Topic 2)
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX 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 127
- (Exam Topic 2)
A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

A. pcap reassembly
B. SSD snapshot

C. Image volatile memory
D. Extract from checksums

Answer: C

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

NEW QUESTION 130
- (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 133
- (Exam Topic 2)
A web server has been compromised due to a ransomware attack. Further Investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago
B. The last known-good configuration stored by the operating system
C. The last full backup that was conducted seven days ago
D. The baseline OS configuration

Answer: A

Explanation:
The last incremental backup that was conducted 72 hours ago would be the best option to restore the services to a secure state, as it would contain the most recent data before the ransomware infection. Incremental backups only store the changes made since the last backup, so they are faster and use less storage space than full backups. Restoring from an incremental backup would also minimize the data loss and downtime caused by the ransomware attack. References:
- https://www.comptia.org/blog/mature-cybersecurity-response-to-ransomware
- https://www.youtube.com/watch?v=HszU4nEAlFc

NEW QUESTION 134
- (Exam Topic 2)
An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan
B. The risk management plan
C. The communication plan
D. The incident response plan

Answer: A

Explanation:
A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

NEW QUESTION 135
- (Exam Topic 2)
A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

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

Answer: B

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

NEW QUESTION 140
- (Exam Topic 2)
A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

A. Install DLP software to prevent data loss.
B. Use the latest version of software.
C. Install a SIEM device.
D. Implement MDM.
E. Implement a screened subnet for the web server.
F. Install an endpoint security solution.
G. Update the website certificate and revoke the existing ones.
H. Deploy additional network sensors.

Answer: BEF

NEW QUESTION 145
- (Exam Topic 2)
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate data center that houses confidential information There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself Which of the following is the weakest design element?

A. The DLP appliance should be integrated into a NGFW.
B. Split-tunnel connections can negatively impact the DLP appliance's performance.
C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

Explanation:
VPN (Virtual Private Network) traffic is encrypted to protect its confidentiality and integrity over the internet. However, this also means that it cannot be inspected by security devices or tools when entering or leaving the network, unless it is decrypted first. This can create a blind spot or a vulnerability for the network security posture, as malicious traffic or data could bypass detection or prevention mechanisms by using VPN encryption

NEW QUESTION 147
- (Exam Topic 2)
Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

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

Answer: C

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

NEW QUESTION 151
- (Exam Topic 2)
A company wants to deploy PKI on its internet-facing website The applications that are currently deployed are
• www company.com (mam website)
• contact us company com (for locating a nearby location)
• quotes company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com Which of the following certificate types would best meet the requirements?

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

Answer: B

Explanation:
A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the

existing applications and any future applications that follow the same naming conventions, such as store.company.com.

NEW QUESTION 155
- (Exam Topic 2)
A user enters a password to log in to a workstation and is then prompted to enter an authentication code Which of the following MFA factors or attributes are being utilized in the authentication process? {Select two).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you know
E. Something you are
F. Something you can do

Answer: AB

Explanation:
MFA (Multi-Factor Authentication) is a method of verifying a user's identity by requiring two or more factors or attributes that belong to different categories. The categories are something you know (such as a password or a PIN), something you have (such as a token or a smart card), something you are (such as a fingerprint or an iris scan), something you do (such as a gesture or a voice command), and somewhere you are (such as a location or an IP address). In this case, the user enters a password (something you know) and then receives an authentication code (something you have) to log in to a workstation.

NEW QUESTION 157
- (Exam Topic 2)
An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

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

Answer: B

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

NEW QUESTION 161
- (Exam Topic 2)
An analyst is concerned about data leaks and wants to restrict access to internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service. Which of the following would be the best technology for the analyst to consider implementing?

A. DLP
B. VPC
C. CASB
D. Content filtering

Answer: C

Explanation:
A cloud access security broker (CASB) is a technology that can restrict access to internet services to authorized users only and control the actions each user can perform on each service. A CASB is a type of software or service that acts as an intermediary between users and cloud service providers. A CASB can enforce security policies, monitor user activity, detect and prevent data leaks, encrypt data, and provide visibility and auditability of cloud usage. References:
https://www.comptia.org/blog/what-is-a-cloud-access-security-broker
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 162
- (Exam Topic 2)
A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

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

Answer: B

Explanation:
Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.
References: 1
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and
Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA

Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3 https://www.comptia.org/blog/what-is-data-loss-prevention

NEW QUESTION 164
- (Exam Topic 2)
An air traffic controller receives a change in flight plan for an morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

A. Mobile hijacking
B. Vishing
C. Unsecure VoIP protocols
D. SPIM attack

Answer: B

Explanation:
Vishing is a form of phishing that uses voice calls or voice messages to trick victims into revealing personal information, such as credit card numbers, bank details, or passwords. Vishing often uses spoofed phone numbers, voice-altering software, or social engineering techniques to impersonate legitimate organizations or authorities. In this scenario, the caller pretended to be someone who could change the flight plan of an aircraft, which could have caused a serious incident.

NEW QUESTION 165
- (Exam Topic 2)
Developers are writing code and merging it into shared repositories several times a day. where it is tested automatically. Which of the following concepts does this best represent?

A. Functional testing
B. Stored procedures
C. Elasticity
D. Continuous Integration

Answer: D

Explanation:
Continuous Integration is the concept that best represents developers writing code and merging it into shared repositories several times a day, where it is tested automatically. Continuous Integration is a software development practice that involves integrating code changes from multiple developers into a shared repository frequently and running automated tests to ensure quality and functionality. Continuous Integration can help to detect and fix errors early, improve collaboration, reduce rework, and accelerate delivery. References: https://www.comptia.org/blog/what-is-devops https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 169
- (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 172
- (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 173
- (Exam Topic 2)
An audit identified Pll being utilized in the development environment of a crit-ical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed: however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to best satisfy both the CPOs and the development team's requirements?

A. Data purge
B. Data encryption
C. Data masking
D. Data tokenization

Answer: D

Explanation:
Data tokenization is a technique of replacing sensitive data with non-sensitive substitutes called tokens that have no intrinsic value or meaning. It can satisfy both the CPO's and the development team's requirements by removing personally identifiable information (PII) from the development environment of a critical application while preserving the functionality and format of the data for testing purposes.

NEW QUESTION 177
- (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)
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

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

Answer: B

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

NEW QUESTION 183
- (Exam Topic 2)
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
* Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?

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

Answer: C

Explanation:

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

- Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin2g3.
- The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on23. This prevents users from copying, changing, or sharing password2s.
- Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness23
. This ensures that passwords are always strong and unpredictable, and reduces the risk of password
reuse or compromise2.
- Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them23. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents2.

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner4. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.
A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification5. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.
A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login6. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 186
- (Exam Topic 2)
Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan

Answer: B

Explanation:
A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented.

NEW QUESTION 188
- (Exam Topic 2)
An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.
Which of the following is the first step the organization should take when implementing the policy?

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

Answer: D

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

NEW QUESTION 191
- (Exam Topic 2)
A security analyst discovers that a company's username and password database were posted on an internet forum. The usernames and passwords are stored in plaintext. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network.
B. Implement salting and hashing.
C. Configure the web content filter to block access to the forum.
D. Increase password complexity requirements.

Answer: B

Explanation:
Salting and hashing are techniques that can improve the security of passwords stored in a database by making them harder to crack or reverse-engineer by hackers who might access the database12.
Salting is the process of adding a unique, random string of characters known only to the site to each password before it is hashed2. Hashing is the process of converting a password into a fixed-length string of characters, which cannot be reversed3. Salting and hashing ensure that the encryption process results in a

different hash value, even when two passwords are the same1. This makes it more difficult for an attacker to use pre-computed tables or dictionaries to guess the passwords, or to exploit duplicate hashes in the database4.

NEW QUESTION 194
- (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 199
- (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 202
- (Exam Topic 2)
A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems. Which Of the following Company most likely complying with?

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

Answer: B

Explanation:
GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization’s systems under certain circumstances. This right is also known as the “right to be forgotten” or the “right to erasure”. An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://gdpr-info.eu/issues/right-to-be-forgotten/

NEW QUESTION 203
- (Exam Topic 2)
A major manufacturing company updated its internal infrastructure and just started to allow OAuth application to access corporate data Data leakage is being reported Which of following most likely caused the issue?

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

Answer: A

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

NEW QUESTION 207
- (Exam Topic 2)
The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

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

Answer: D

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

NEW QUESTION 209
- (Exam Topic 2)
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

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

Answer: BC

Explanation:
A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service1. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability2. A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization’s users3. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.
References: 1: https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/ 2: https://www.imperva.com/learn/application-security/load-balancing/ 3: https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/ : https://www.imperva.com/learn/application-security/vpn-virtual-private-network/ : https://www.imperva.com/learn/application-security/transport-layer-security-tls/ : https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/ : https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins
: https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall : https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur

NEW QUESTION 214
- (Exam Topic 2)
Which of the following threat actors is most likely to be motivated by ideology?

A. Business competitor
B. Hacktivist
C. Criminal syndicate
D. Script kiddie
E. Disgruntled employee

Answer: B

Explanation:
A hacktivist is a threat actor who is most likely to be motivated by ideology. A hacktivist is a person or group who uses hacking skills and techniques to promote a political or social cause. Hacktivists may target government, corporate, or religious entities that they disagree with or oppose. Hacktivists may use various methods to achieve their goals, such as defacing websites, leaking sensitive data, launching denial-of-service attacks, or spreading propaganda. Hacktivists are not motivated by financial gain or personal benefit, but rather by their beliefs and values. References:
- https://www.uscybersecurity.net/hacktivist/
- https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

NEW QUESTION 218
- (Exam Topic 2)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator

D. Data custodian
E. Internal auditor

Answer: C

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

NEW QUESTION 221
- (Exam Topic 2)
A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

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

Answer: A

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

NEW QUESTION 224
- (Exam Topic 2)
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 227
- (Exam Topic 2)
An organization is repairing damage after an incident. Which Of the following controls is being implemented?

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

Answer: C

Explanation:
Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions

such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

NEW QUESTION 232
- (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 237
- (Exam Topic 2)
A security analyst is reviewing packet capture data from a compromised host On the In the packet capture. analyst locates packets that contain large of text, Which Of following is most likely installed on compromised host?

A. Keylogger
B. Spyware
C. Torjan
D. Ransomware

Answer: A

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

NEW QUESTION 240
- (Exam Topic 2)
An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

A. Intrusion prevention system
B. Proxy server
C. Jump server
D. Security zones

Answer: A

Explanation:
An intrusion prevention system (IPS) is the best solution to implement on the company’s network to detect and prevent suspicious attempts to access company resources. An IPS is a network security technology that continuously monitors network traffic for malicious or anomalous activity and takes automated actions to block or mitigate it. An IPS can also alert the system administrators of any potential threats and provide detailed logs and reports of the incidents. An IPS can help the company to improve its security posture and prevent data breaches, unauthorized access, or denial-of-service attacks. References:
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

NEW QUESTION 243
- (Exam Topic 2)
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

A. SED
B. HSM
C. DLP
D. TPM

Answer: A

Explanation:
SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine1.

SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

NEW QUESTION 247
- (Exam Topic 2)
An annual information security assessment 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 249
- (Exam Topic 2)
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 254
- (Exam Topic 2)
Two organizations are discussing a possible merger Both Organizations Chief Fi-nancial Officers would like to safely share payroll data with each Other to de-termine if the pay scales for different roles are similar at both organizations Which Of the following techniques would be best to protect employee data while allowing the companies to successfully share this information?

A. Pseudo-anonymization
B. Tokenization
C. Data masking
D. Encryption

Answer: A

Explanation:
Pseudo-anonymization is a technique of replacing sensitive data with artificial identifiers or pseudonyms that preserve some characteristics or attributes of the original data. It can protect employee data while allowing the companies to successfully share this information by removing direct identifiers such as names, addresses, etc., but retaining indirect identifiers such as job roles, pay scales, etc., that are relevant for the comparison.

NEW QUESTION 256
- (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 257
- (Exam Topic 2)

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

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

Answer: DF

Explanation:
A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.
To determine the sequence of a server farm's logs, the administrator should consider the following factors:
- Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.
- Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

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

NEW QUESTION 258
- (Exam Topic 2)
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 261
- (Exam Topic 2)
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 265
- (Exam Topic 2)
Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan
B. Threat intelligence
C. Log aggregation
D. Packet capture

Answer: D

Explanation:
- Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities
- Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses
- Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling
- Using a CASB tool to control access to cloud resources and prevent data leaks or downloads
- Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

NEW QUESTION 269
- (Exam Topic 2)

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 271
- (Exam Topic 2)
A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

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

Answer: C

Explanation:
Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

NEW QUESTION 272
- (Exam Topic 2)
A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

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

Answer: B

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

NEW QUESTION 274
- (Exam Topic 2)
A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors Of real-world events in order to improve the incident response team's process. Which Of the following is the analyst most likely participating in?

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

Answer: A

Explanation:

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

NEW QUESTION 278
- (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 283
- (Exam Topic 2)
During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production Which of the following describes what the company should do first to lower the risk to the
Production the hardware.

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

Answer: B

Explanation:
Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. References: 1
CompTIA Security+
Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize
secure application development, deployment, and automation concepts 2
CompTIA Security+ Certification
Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of
embedded and specialized systems security 3 https://www.comptia.org/blog/patch-management-best-practices

NEW QUESTION 284
- (Exam Topic 2)
Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

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

Answer: C

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

NEW QUESTION 287
- (Exam Topic 2)
A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access pcints are up and running. One of the help desk technicians notices the affected users are working in a near the parking Jot Which Of the following IS the most likely reason for the outage?

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

Answer: A

Explanation:
Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

NEW QUESTION 290
- (Exam Topic 2)
Which of the following should customers who are involved with Ul 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 Ul 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 294
- (Exam Topic 2)
A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

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

Answer: B

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

NEW QUESTION 298
- (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 303
- (Exam Topic 2)
During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

A. Legacy operating system
B. Weak configuration
C. Zero day
D. Supply chain

Answer: C

Explanation:
A zero-day vulnerability is a security flaw that is unknown to the vendor and the public, and therefore has no patch or fix available. A zero-day attack is an exploit that takes advantage of a zero-day vulnerability before the vendor or the security community becomes aware of it. A zero-day attack can cause serious damage to a system or network, as there is no defense against it until a patch is released. References:
- https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/
- https://www.professormesser.com/security-plus/sy0-501/zero-day-attacks-4/

NEW QUESTION 307
- (Exam Topic 2)
An organization decided not to put controls in place because of the high cost of implementing the controls compared to the cost of a potential fine. Which of the following risk management strategies is the organization following?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

Answer: D

Explanation:
Acceptance is a risk management strategy that involves acknowledging the existence and potential impact of a risk, but deciding not to take any action to reduce or eliminate it. This strategy is usually adopted when the cost of implementing controls outweighs the benefit of mitigating the risk, or when the risk is deemed acceptable or unavoidable. In this case, the organization decided not to put controls in place because of the high cost compared to the potential fine, which means they accepted the risk. References: https://www.comptia.org/blog/what-is-risk-acceptance

NEW QUESTION 308
- (Exam Topic 2)
A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away. Which of the following solutions should the CISO implement?

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

Answer: B

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

NEW QUESTION 309
- (Exam Topic 2)
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

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

Answer: C

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 312
- (Exam Topic 2)
An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation Which of the following method did attacker to insert the contacts without having 'Physical access to device?

A. Jamming
B. BluJacking
C. Disassoaatm
D. Evil twin

Answer: B

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

NEW QUESTION 314
- (Exam Topic 2)
A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software
C. Performing static code analysis on the software
D. Ensuring secure cookies are used

Answer: B

Explanation:
Code signing is a cryptographic process that allows software developers to digitally sign their code. This ensures that the code has not been tampered with since it was signed and that it came from a trusted source.
Testing input validation on the user input fields is important for preventing malicious code from being entered into a system. However, it does not address the authenticity of the code itself.
Performing static code analysis on the software can help to identify security vulnerabilities. However, it cannot guarantee that the code has not been tampered with.
Ensuring secure cookies are used is important for preventing unauthorized access to user data. However, it does not address the authenticity of the code itself.
Therefore, the most appropriate option to ensure the authenticity of the code created by the company is to perform code signing on the software.
Here are some additional benefits of code signing:

- It can help to prevent malware from being installed on users' computers.
- It can help to protect intellectual property.
- It can help to improve user trust.

NEW QUESTION 317
- (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 318
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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