Exam Questions SY0-701

CompTIA Security+ Exam

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

NEW QUESTION 1
- (Exam Topic 1)
An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

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

Answer: B

Explanation:
EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 2
- (Exam Topic 1)
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

A. privilege escalation
B. footprinting
C. persistence
D. pivoting.

Answer: D

Explanation:
The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting.
References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Enumeration and Penetration Testing

NEW QUESTION 3
- (Exam Topic 1)
Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

A. Test
B. Staging
C. Development
D. Production

Answer: A

Explanation:
The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics. References: CompTIA Security+ Study Guide 601, Chapter 2

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

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

Answer: B

Explanation:
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.
An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION 6
- (Exam Topic 1)
The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

Answer: C

Explanation:
To prevent such a breach in the future, the BEST control to use would be Password complexity.
Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.
The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough. References:
CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 7
- (Exam Topic 1)
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter
B. SIEM
C. Firewall rules
D. DLP

Answer: C

Explanation:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

NEW QUESTION 8
- (Exam Topic 1)
Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing

Answer: B

Explanation:
Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life1. Shredding reduces electronic devices to pieces no larger than 2 millimeters2. Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
A company acquired several other small companies The company thai acquired the others is transitioning network services to the cloud The company wants to make sure that performance and security remain intact Which of the following BEST meets both requirements?

A. High availability
B. Application security
C. Segmentation
D. Integration and auditing

Answer: A

Explanation:
High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

NEW QUESTION 10
- (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 13
- (Exam Topic 1)
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving
B. Shoulder surfing
C. Information elicitation
D. Credential harvesting

Answer: A

Explanation:
Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.
References:
- CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

NEW QUESTION 16
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

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

Answer: A

Explanation:
Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and

proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

NEW QUESTION 21
- (Exam Topic 1)
During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow
B. Pass the hash
C. SQL injection
D. Replay attack

Answer: B

Explanation:
Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

NEW QUESTION 23
- (Exam Topic 1)
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

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

Answer: D

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

NEW QUESTION 28
- (Exam Topic 1)
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
Which of the following documents did Ann receive?

A. An annual privacy notice
B. A non-disclosure agreement
C. A privileged-user agreement
D. A memorandum of understanding

Answer: A

Explanation:
Ann received an annual privacy notice from her mortgage company. An annual privacy notice is a statement from a financial institution or creditor that outlines the institution's privacy policy and explains how the institution collects, uses, and shares customers' personal information. It informs the customer about their rights under the Gramm-Leach-Bliley Act (GLBA) and the institution's practices for protecting their personal information. References:
- CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 29
- (Exam Topic 1)
Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

Explanation:
When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 34
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system,

selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framevtoik
D. ISO 27002

Answer: C

Explanation:
The CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system. The RMF is a structured process for managing risks that involves categorizing the system, selecting controls, implementing controls, assessing controls, and authorizing the system.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 4: Risk Management, pp. 188-191.

NEW QUESTION 35
- (Exam Topic 1)
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

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

Answer: B

Explanation:
Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

NEW QUESTION 37
- (Exam Topic 1)
Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps
B. Security guards
C. Video surveillance
D. Fences
E. Bollards
F. Antivirus

Answer: AB

Explanation:
A - a mantrap can trap those personnal with bad intension(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnal from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnal from entering(preventive+deterrent), and notice those personnal as well(detective)

NEW QUESTION 39
- (Exam Topic 1)
Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed,
agreed-upon duration of time?

A. PoC
B. Production
C. Test
D. Development

Answer: A

Explanation:
A proof of concept (PoC) environment can be stood up quickly and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time. This environment can utilize either dummy data or actual data. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 42
- (Exam Topic 1)
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

Answer: A

Explanation:
The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.

NEW QUESTION 43
- (Exam Topic 1)
A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

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

Answer: A

Explanation:
To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and
decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic. References:
- CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 44
- (Exam Topic 1)
A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain
B. Domain hijacking
C. DNS poisoning
D. URL redirection

Answer: C

Explanation:
The log entry shows the IP address for "www.example.com" being changed to a different IP address, which is likely the result of DNS poisoning. DNS poisoning occurs when an attacker is able to change the IP address associated with a domain name in a DNS server's cache, causing clients to connect to the attacker's server instead of the legitimate server. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 48
- (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 49
- (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 53
- (Exam Topic 1)
A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?

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

Answer: C

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

NEW QUESTION 54
- (Exam Topic 1)
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps
B. A Telnet session
C. An SSH connection
D. SFTP traffic

Answer: B

Explanation:
The security analyst is likely observing a Telnet session, as Telnet transmits data in plain text format, including usernames and passwords. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware.

NEW QUESTION 56
- (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 60
- (Exam Topic 1)
The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

A. prepending.
B. an influence campaign.
C. a watering-hole attack.
D. intimidation.
E. information elicitation.

Answer: B

Explanation:
This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

NEW QUESTION 63
- (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 65
- (Exam Topic 1)
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images
B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
C. Define a vulnerability scan to assess container images before being introduced on the environment
D. Create a dedicated VPC for the containerized environment

Answer: A

Explanation:
Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 11: Cloud Security, Container Security

NEW QUESTION 69
- (Exam Topic 1)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity

Answer: B

Explanation:
A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 73
- (Exam Topic 1)
The help desk has received calls from users in multiple locations who are unable to access core network services The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?

A. Disconnect all external network connections from the firewall
B. Send response teams to the network switch locations to perform updates
C. Turn on all the network switches by using the centralized management software
D. Initiate the organization's incident response plan.

Answer: D

Explanation:
An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.
If the help desk has received calls from users in multiple locations who are unable to access core network services, it could indicate that a network outage or a denial-of-service attack has occurred. The network team has identified and turned off the network switches using remote commands, which could be a containment measure to isolate the affected devices and prevent further damage.
The next action that the network team should take is to initiate the organization’s incident response plan, which would involve notifying the appropriate stakeholders, such as management, security team, legal team, etc., and following the predefined steps to investigate, analyze, document, and resolve the incident.
The other options are not correct because:
- A. Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.
- B. Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.
- C. Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.

According to CompTIA Security+ SY0-601 Exam Objectives 1.5 Given a scenario, analyze indicators of compromise and determine the type of malware:
“An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.”
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives

NEW QUESTION 77
- (Exam Topic 1)
A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been Which of the following statements BEST explains the issue?

A. OpenID is mandatory to make the MFA requirements work
B. An incorrect browser has been detected by the SAML application
C. The access device has a trusted certificate installed that is overwriting the session token
D. The user's IP address is changing between logins, bur the application is not invalidating the token

Answer: D

NEW QUESTION 82
- (Exam Topic 1)
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

A. whaling.
B. smishing.
C. spear phishing
D. vishing

Answer: C

Explanation:
The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

NEW QUESTION 87
- (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:
Detailed
Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p. 465

NEW QUESTION 88
- (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 92
- (Exam Topic 1)
Which of the following conditions impacts data sovereignty?

A. Rights management
B. Criminal investigations
C. Healthcare data
D. International operations

Answer: D

Explanation:

Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. References:
- CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 93
- (Exam Topic 1)
Which of the following roles would MOST likely have direct access to the senior management team?

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

Answer: C

Explanation:
A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders.
A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.
The other options are not correct because:
- A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
- B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
- D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:
“A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization.”
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://gdpr-info.eu/issues/data-protection-officer/

NEW QUESTION 94
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

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

Answer: B

Explanation:
A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION 95
- (Exam Topic 1)
A company is concerned about individuals dnvmg a car into the building to gam access Which of the following security controls would work BEST to prevent this from happening?

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

Answer: A

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

NEW QUESTION 98
- (Exam Topic 1)
During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics
B. Dump files
C. Bandwidth monitors
D. Protocol analyzer output

Answer: A

Explanation:
User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 338-341

NEW QUESTION 99
- (Exam Topic 1)
A company recently experienced an attack during which 5 main website was directed to the atack-er's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company Implement to prevent this type of attack from occurring in the future?

A. IPSec
B. SSL/TLS
C. DNSSEC
D. S/MIME

Answer: C

Explanation:
The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.
To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC.
DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

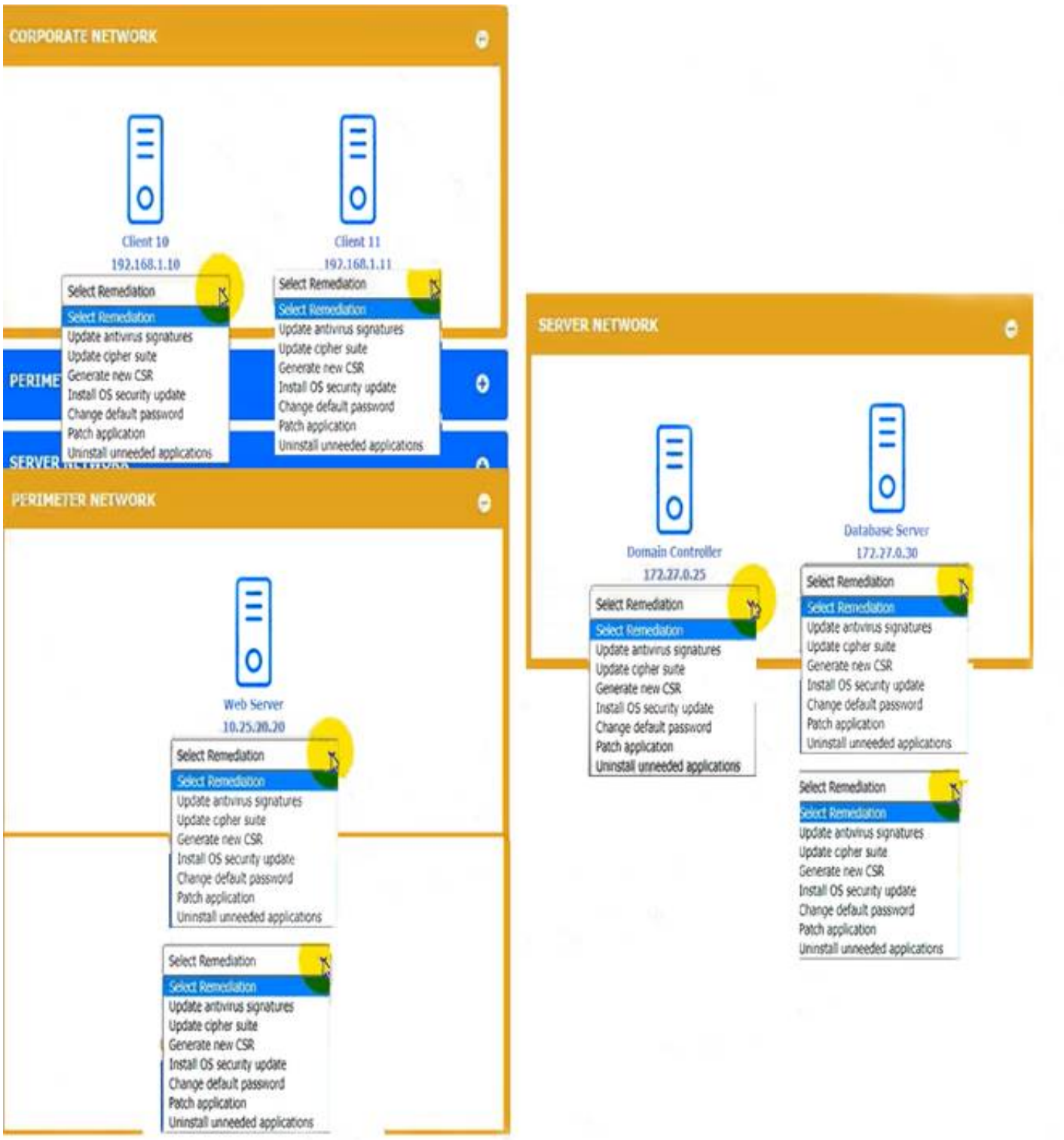
NEW QUESTION 100
- (Exam Topic 1)
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

Answer: A

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

NEW QUESTION 102
- (Exam Topic 1)
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce. Remediation options may be selected multiple times, and some devices may require more than one
remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.

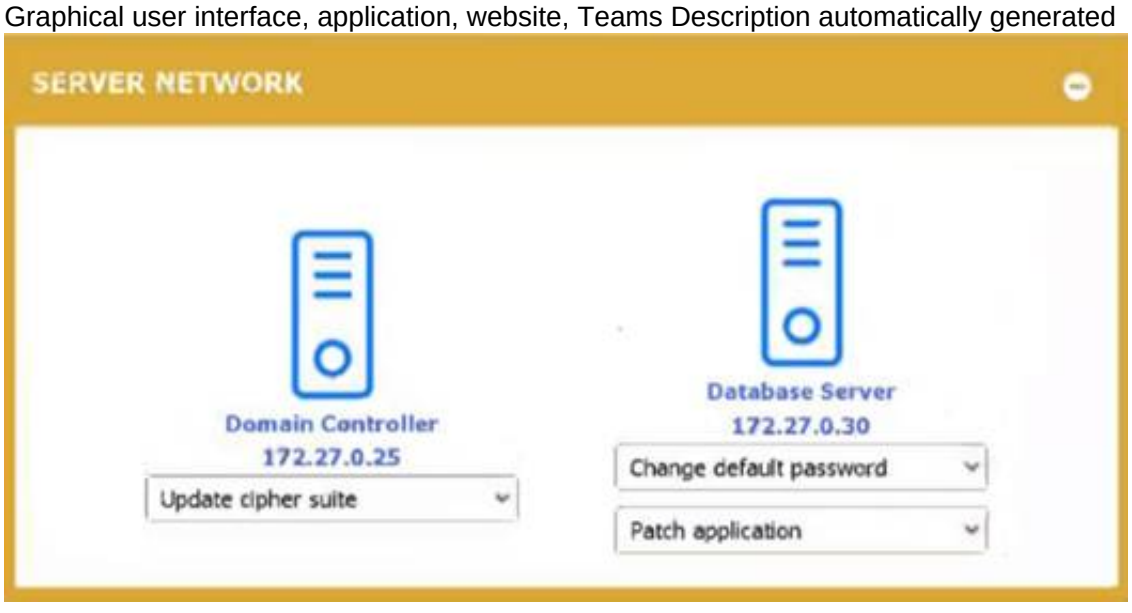


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, website, Teams Description automatically generated



Graphical user interface, text, application Description automatically generated

NEW QUESTION 103
- (Exam Topic 1)
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

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

Answer: D

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

NEW QUESTION 106
- (Exam Topic 1)
A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?

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

Answer: B

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

NEW QUESTION 109
- (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 111
- (Exam Topic 1)
During an incident a company CIRT determine it is necessary to observe the continued network-based transaction 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 risk of lateral spread and the risk that the adversary would notice any changes?

A. Physical move the PC to a separate internet pint of presence
B. Create and apply micro segmentation rules.
C. Emulate the malware in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:
To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral

spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary. References: https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/

NEW QUESTION 116
- (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 118
- (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 123
- (Exam Topic 2)
A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are
being transmitted and stored more securely?

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

Answer: B

Explanation:
Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.
A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION 127
- (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 132
- (Exam Topic 2)
An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to Implement mitigation techniques to prevent further spread. Which of the
following is the best course of action for the analyst to take?

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

Answer: D

Explanation:
Isolating the infected attachment is the best course of action for the analyst to take to prevent further spread of the worm. A worm is a type of malware that can self-replicate and infect other devices without human interaction. By isolating the infected attachment, the analyst can prevent the worm from spreading to other devices or networks via email, file-sharing, or other means. Isolating the infected attachment can also help the analyst to analyze the worm and determine its source, behavior, and impact. References:
- https://www.security.org/antivirus/computer-worm/
- https://sec.cloudapps.cisco.com/security/center/resources/worm_mitigation_whitepaper.html

NEW QUESTION 135
- (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 139
- (Exam Topic 2)
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective

Answer: B

Explanation:
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION 143
- (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 146
- (Exam Topic 2)
Which of the following would be used to find the most common web-applicalion vulnerabilities?

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

Answer: A

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

NEW QUESTION 148
- (Exam Topic 2)
Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

A. Edge computing
B. Microservices
C. Containers
D. Thin client

Answer: C

Explanation:
Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

NEW QUESTION 153
- (Exam Topic 2)
An organization has hired a security analyst to perform a penetration test The analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. CURL
C. Neat
D. Wireshark

Answer: D

Explanation:
Wireshark is a tool that can analyze pcap files, which are files that capture network traffic. Wireshark can display the packets, protocols, and other details of the network traffic in a graphical user interface. Nmap is a tool that can scan networks and hosts for open ports and services. CURL is a tool that can transfer data from or to a server using various protocols. Neat is a tool that can test network performance and quality.

NEW QUESTION 156
- (Exam Topic 2)
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. laaS
D. DaaS

Answer: C

Explanation:
laaS (Infrastructure as a Service) is a cloud model that provides clients with servers, storage, and networks but nothing else. It allows clients to have more control and flexibility over the configuration and management of their infrastructure resources, but also requires them to install and maintain their own operating systems, applications, etc.

NEW QUESTION 161
- (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 164
- (Exam Topic 2)
An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using Which Of the following would be best to use to update and reconfigure the OS.level security configurations?

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

Answer: A

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

NEW QUESTION 166
- (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 168
- (Exam Topic 2)
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the ‘company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

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

Answer: AF

Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple applications or services that trust the same identity provider. Open authentication is a standard protocol that enables federation by allowing users to use their existing credentials from one service to access another service. The company is most likely using federation and open authentication to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account. For example, the company could use an identity provider such as Azure AD or Keycloak to manage the user identities and credentials for the intranet account, and then use open authentication to allow the users to access other company-owned websites without having to log in again. References:
- https://www.keycloak.org/
- https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed

NEW QUESTION 173
- (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 178
- (Exam Topic 2)
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?

A. SOC2
B. CSA
C. CSF
D. 1SO 31000

Answer: A

Explanation:
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3: https://www.csagroup.org/store/product/50072454os/ 1: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

NEW QUESTION 182
- (Exam Topic 2)
A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server In order to validate current employees. Which of the following should the systems integrator configure to be the most secure?

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

Answer: D

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

NEW QUESTION 183
- (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 185
- (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 189
- (Exam Topic 2)
A data cento has experienced an increase in under-voltage events Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability Which of the following would be the most cost-effective solution for the data center 10 implement"

A. Uninterruptible power supplies with battery backup
B. Managed power distribution units lo track these events
C. A generator to ensure consistent, normalized power delivery
D. Dual power supplies to distribute the load more evenly

Answer: A

Explanation:
Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes. References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.apc.com/us/en/faqs/FA158852/

NEW QUESTION 193
- (Exam Topic 2)
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.

Answer: B

Explanation:
Data is being exfiltrated when an internal system is sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Data exfiltration is the unauthorized transfer of data from a system or network to an external destination or actor. Data exfiltration can be performed by malicious insiders or external attackers who have compromised the system or network. DNS queries are requests for resolving domain names to IP addresses. DNS queries can be used as a covert channel for data exfiltration by encoding data in the domain names or subdomains and sending them to a malicious DNS server that can decode and collect the data. References:
https://www.comptia.org/blog/what-is-data-exfiltration
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 198
- (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 202
- (Exam Topic 2)
A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

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

Answer: BD

Explanation:
* B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. References: 1
CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1 : Explain the importance of secure staging deployment concepts 2
CompTIA Security+ Certification Exam
Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application
development, deployment, and automation concepts 3
CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

NEW QUESTION 205
- (Exam Topic 2)
A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID
B. UPS
C. NIC teaming
D. Load balancing

Answer: C

Explanation:
NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:
https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 207
- (Exam Topic 2)
An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

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

Answer: D

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

NEW QUESTION 208
- (Exam Topic 2)
Which Of the following best ensures minimal downtime for organizations vÄh crit-ical computing equipment located in earthquake-prone areas?

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

Answer: B

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

NEW QUESTION 209
- (Exam Topic 2)
Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

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

Answer: B

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

NEW QUESTION 213
- (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 215
- (Exam Topic 2)
A security team will be outsourcing several key functions to a third party and will require that:
• Several of the functions will carry an audit burden.
• Attestations will be performed several times a year.
• Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

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

Answer: C

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

NEW QUESTION 218
- (Exam Topic 2)
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
A screenshot of a computer program Description automatically generated with low confidence

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

NEW QUESTION 223
- (Exam Topic 2)
A security administrator is using UDP port 514 to send a syslog through an unsecure network to the SIEM server. Which of the following is the best way for the administrator to improve the process?

A. Change the protocol to TCP.
B. Add LDAP authentication to the SIEM server.
C. Use a VPN from the internal server to the SIEM and enable DLP.
D. Add SSL/TLS encryption and use a TCP 6514 port to send logs.

Answer: D

Explanation:
SSL/TLS encryption is a method of securing the syslog traffic by using cryptographic protocols to encrypt and authenticate the data. SSL/TLS encryption can prevent eavesdropping, tampering, or spoofing of the syslog messages. TCP 6514 is the standard port for syslog over TLS, as defined by RFC 5425. Using this port can ensure compatibility and interoperability with other syslog implementations that support TLS.

NEW QUESTION 224
- (Exam Topic 2)
A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

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

Which of the following password attacks is taking place?

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

Answer: D

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

NEW QUESTION 227
- (Exam Topic 2)
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would best describe the estimated number of devices to be replaced next year?

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

Answer: B

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

NEW QUESTION 230
- (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 235
- (Exam Topic 2)
The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:
• Minimal interruption to the end user
• Mutual certificate validation
Which of the following authentication protocols would meet these requirements?

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

Answer: D

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

NEW QUESTION 238
- (Exam Topic 2)
A company recently suffered a breach in which an attacker was able to access the internal mail servers and directly access several user inboxes. A large number of email messages were later posted online. Which of the following would bast prevent email contents from being released should another breach occur?

A. Implement S/MIME to encrypt the emails at rest.
B. Enable full disk encryption on the mail servers.
C. Use digital certificates when accessing email via the web.
D. Configure web traffic to only use TLS-enabled channels.

Answer: A

Explanation:
S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which is a standard for encrypting and digitally signing email messages. S/MIME can provide confidentiality, integrity, authentication and
non-repudiation for email communications. S/MIME can encrypt the emails at rest, which means that the
email contents are protected even if they are stored on the mail servers or the user inboxes. S/MIME can prevent email contents from being released should another breach occur, as the attacker would not be able to decrypt or read the encrypted emails without the proper keys or certificates. Verified References:
- Cryptography Concepts – SY0-601 CompTIA Security+ : 2.8 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/cryptography-concepts-2/ (See
S/MIME)
- Mail Encryption - CompTIA Security+ All-in-One Exam Guide (Exam SY0-301) https://www.oreilly.com/library/view/comptia-security-all-in-one/9780071771474/sec5_chap14.html (See S/MIME)
- Symmetric and Asymmetric Encryption – CompTIA Security+ SY0-501 – 6.1 https://www.professormesser.com/security-plus/sy0-501/symmetric-and-asymmetric-encryption/ (See S/MIME)

NEW QUESTION 241
- (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 points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

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

Answer: A

Explanation:
Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

NEW QUESTION 246
- (Exam Topic 2)
A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.
Which of the following should the security operations center implement?

A. theHarvester
B. Nessus

C. Cuckoo
D. Sn1per

Answer: C

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

NEW QUESTION 250
- (Exam Topic 2)
A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

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

Answer: A

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

NEW QUESTION 252
- (Exam Topic 2)
A security administrator examines the ARP table of an access switch and sees the following output:

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

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

A. DDoSonFa02 port
B. MAG flooding on Fa0/2 port
C. ARP poisoning on Fa0/1 port
D. DNS poisoning on port Fa0/1

Answer: C

Explanation:
ARP poisoning is a type of attack that exploits the ARP protocol to associate a malicious MAC address with a legitimate IP address on a network1. This allows the attacker to intercept, modify or drop traffic between the victim and other hosts on the same network. In this case, the ARP table of the access switch shows that the same MAC address (00-0c-29-58-35-3b) is associated with two different IP addresses (192.168.1.100 and 192.168.1.101) on port Fa0/12. This indicates that an attacker has poisoned the ARP table to redirect traffic intended for 192.168.1.100 to their own device with MAC address 00-0c-29-58-35-3b. The other options are not related to this scenario. DDoS is a type of attack that overwhelms a target with excessive traffic from multiple sources3. MAC flooding is a type of attack that floods a switch with fake MAC addresses to exhaust its MAC table and force it to operate as a hub4. DNS poisoning is a type of attack that corrupts the DNS cache with fake entries to redirect users to malicious websites.
References: 1: https://www.imperva.com/learn/application-security/arp-spoofing/ 2: https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148 3: https://www.imperva.com/learn/application-security/ddos-attack/ 4: https://www.imperva.com/learn/application-security/mac-flooding/ : https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/

NEW QUESTION 253
- (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 254
- (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 259
- (Exam Topic 2)
A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

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

Answer: A

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

NEW QUESTION 261
- (Exam Topic 2)
A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output

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

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

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

Answer: C

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

NEW QUESTION 262

- (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 265
- (Exam Topic 2)
Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ether ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

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

Answer: A

Explanation:
NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

NEW QUESTION 266
- (Exam Topic 2)
A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

A. DLP
B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF

Answer: CD

Explanation:
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

NEW QUESTION 269

- (Exam Topic 2)
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

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

Answer: D

Explanation:
Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 274
- (Exam Topic 2)
A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. Which of the following concepts should the administrator utilize?

A. Provisioning
B. Staging
C. Development
D. Quality assurance

Answer: A

Explanation:
Provisioning is the process of creating and setting up IT infrastructure, and includes the steps required to manage user and system access to various resources . Provisioning can be done for servers, cloud environments, users, networks, services, and more .
In this case, the security administrator wants to ensure that all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. This means that the administrator needs to
provision the cloud servers with the necessary software and configuration before they are deployed or used by customers or end users. Provisioning can help automate and standardize the process of setting up cloud servers and reduce the risk of human errors or inconsistencies.

NEW QUESTION 276
- (Exam Topic 2)
Which of the following allow access to remote computing resources, a operating system. and centrdized configuration and data

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

Answer: C

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

NEW QUESTION 280
- (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 284
- (Exam Topic 2)
Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP

B. CSR
C. CA
D. CRC

Answer: A

Explanation:
Online Certificate Status Protocol (OCSP) is used to validate a certificate when it is presented to a user. OCSP is a protocol that allows a client or browser to query the status of a certificate from an OCSP responder, which is a server that maintains and provides the revocation status of certificates issued by a certificate authority (CA). OCSP can help to verify the authenticity and validity of a certificate and prevent the use of revoked or expired certificates. References:
https://www.comptia.org/blog/what-is-ocsp
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 287
- (Exam Topic 2)
Which of the following terms should be included in a contract to help a company monitor the ongo-ing security maturity Of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to kept for a minimum of 30 days
C. Integration of threat intelligence in the companys AV
D. A data-breach clause requiring disclosure of significant data loss

Answer: A

Explanation:
A right-to-audit clause is a contractual provision that allows one party to audit the records and activities of
another party to ensure compliance with security policies and standards. It can help a company monitor the ongoing security maturity of a new vendor by conducting annual security audits and identifying any gaps or issues that need to be addressed.

NEW QUESTION 289
- (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 290
- (Exam Topic 2)
Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?

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

Answer: C

Explanation:
Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.atlassian.com/git/tutorials/what-is-version-control

NEW QUESTION 292
- (Exam Topic 2)
A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner, Which of the following concepts describes this scenario?

A. Red-team exercise
B. Business continuity plan testing
C. Tabletop exercise
D. Functional exercise

Answer: C

Explanation:

A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it1. A tabletop exercise is a low-impact and
cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and
enhance communication and coordination among team members2. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization3. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption4. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.
References: 1:
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g
2: https://www.linuxjournal.com/content/security-exercises 3:
https://www.imperva.com/learn/application-security/red-team-blue-team/ 4: https://www.ready.gov/business-continuity-plan : https://www.ready.gov/exercises

NEW QUESTION 294
- (Exam Topic 2)
A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

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

Answer: AF

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

NEW QUESTION 298
- (Exam Topic 2)
Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification
B. Accountability
C. Legal hold
D. Chain of custody

Answer: C

Explanation:
A legal hold is a process that requires an organization to preserve electronically stored information and paper documents that are relevant to a pending or anticipated litigation or investigation. It suspends the normal retention and destruction policies and procedures for such information and documents until the legal hold is lifted or released.

NEW QUESTION 302
- (Exam Topic 2)
Which of the following security controls s sed to isolate a section of the network and its externally available resources from the internal corporate network in order to reduce the number of
possible attacks?

A. Faraday cages
B. Air gap
C. Vaulting
D. Proximity readers

Answer: B

Explanation:
An air gap is a security measure that physically isolates a section of the network from any other network or device that could compromise its security. An air gap prevents any unauthorized access, data leakage, or malware infection through network connections, such as Ethernet cables, wireless signals, or Bluetooth devices. An air gap can be used to protect sensitive or critical systems and data from external threats, such as hackers, spies, or cyberattacks.

NEW QUESTION 307
- (Exam Topic 2)
Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

A. Public cloud
B. Hybrid cloud
C. Community cloud
D. Private cloud

Answer: A

Explanation:
There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.
According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION 309
- (Exam Topic 2)
A security professional wants to enhance the protection of a critical environment that is Used to store and manage a company's encryption keys. The selected technology should be tamper resistant. Which of the following should the security professional implement to achieve the goal?

A. DLP
B. HSM
C. CA
D. FIM

Answer: B

Explanation:
HSM stands for hardware security module, which is a physical device that is used to store and manage cryptographic keys in a secure and tamper-resistant manner. HSMs can provide high-performance encryption and decryption operations, as well as key generation, backup, and recovery. HSMs can also prevent unauthorized access or extraction of the keys, even by the cloud service provider or the HSM vendor. HSMs can enhance the protection of a critical environment that is used to store and manage encryption keys for a financial institution or any other organization that deals with sensitive data. References:
- https://www.comptia.org/certifications/security
- https://www.professormesser.com/security-plus/sy0-501/hardware-security-3/

NEW QUESTION 314
- (Exam Topic 2)
A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.
Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?

A. NIDS
B. MAC filtering
C. Jump server
D. IPSec
E. NAT gateway

Answer: C

Explanation:
A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.

NEW QUESTION 318
- (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 319
- (Exam Topic 2)
An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's need?

A. MFA
B. 802.1X
C. WPA2
D. TACACS

Answer: B

Explanation:
* 802.1 X is a standard for network access control that provides authentication and encryption for devices that connect to a LAN/WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (the device requesting access), an authenticator (the device granting access), and an authentication server (the device verifying credentials). 802.1X can prevent on-path attacks and evil twin attacks by requiring users to

provide valid credentials before accessing the network and encrypting the data transmitted over the network.
On-path attacks are attacks that involve intercepting or modifying network traffic between two endpoints. An on-path attacker can eavesdrop on sensitive information, alter or inject malicious data, or redirect traffic to malicious destinations. On-path attacks are frequently perpetrated over WiFi network1s.
Evil twin attacks are attacks that involve setting up a fake WiFi access point that mimics a legitimate one. An evil twin attacker can trick users into connecting to the fake network and then monitor or manipulate their online activity. Evil twin attacks are more common on public WiFi networks that are unsecured and leave personal data vulnerable23.

NEW QUESTION 322
- (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 326
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

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

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

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