



# CompTIA

## Exam Questions SY0-701

CompTIA Security+ Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

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

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

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

### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:

> CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

### NEW QUESTION 2

- (Exam Topic 1)

A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- \* www.companysite.com
- \* shop.companysite.com
- \* about-us.companysite.com
- \* contact-us.companysite.com
- \* secure-login.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate
- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate
- E. An extended validation certificate

**Answer: D**

#### Explanation:

The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.

The retail company should use a wildcard certificate if it is concerned with convenience and cost. A wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (\*) in the domain name field, and can secure multiple subdomains of the primary domain.

### NEW QUESTION 3

- (Exam Topic 1)

Which of the following would produce the closest experience of responding to an actual incident response scenario?

- A. Lessons learned
- B. Simulation
- C. Walk-through
- D. Tabletop

**Answer: B**

#### Explanation:

A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident. References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

### NEW QUESTION 4

- (Exam Topic 1)

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?

- A. Functional testing
- B. Stored procedures
- C. Elasticity
- D. Continuous integration

**Answer: D**

#### Explanation:

Continuous integration is a software development practice where developers merge their code into a shared repository several times a day, and the code is tested automatically. This ensures that code changes are tested and integrated continuously, reducing the risk of errors and conflicts.

### NEW QUESTION 5

- (Exam Topic 1)

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at

Layer 7? (Select TWO).

- A. HIDS
- B. NIPS
- C. HSM
- D. WAF
- E. NAC
- F. NIDS
- G. Stateless firewall

**Answer:** DF

**Explanation:**

A WAF (Web Application Firewall) and NIDS (Network Intrusion Detection System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIDS can also detect attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors. References: CompTIA Security+ Study Guide, pages 94-95, 116-118

**NEW QUESTION 6**

- (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 7**

- (Exam Topic 1)

A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication
- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

**Answer:** B

**Explanation:**

The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true. References: CompTIA Security+ SY0-601 Exam Objectives: 3.1 Given a scenario, use appropriate software tools to assess the security posture of an organization.

**NEW QUESTION 8**

- (Exam Topic 1)

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

- A. Privacy
- B. Cloud storage of telemetry data
- C. GPS spoofing
- D. Weather events

**Answer:** A

**Explanation:**

The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated. References:

> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

**NEW QUESTION 9**

- (Exam Topic 1)

Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

- A. Penetration testing
- B. Code review
- C. Wardriving
- D. Bug bounty

**Answer:** D

**Explanation:**

A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook), Google, Microsoft, and others to improve the security of their products and services. Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

**NEW QUESTION 10**

- (Exam Topic 1)

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

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

**Answer: C**

**Explanation:**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

**NEW QUESTION 10**

- (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 11**

- (Exam Topic 1)

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

- A. SIEM
- B. SOAR
- C. EDR
- D. CASB

**Answer: B**

**Explanation:**

Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

**NEW QUESTION 16**

- (Exam Topic 1)

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept includes granting logical access based on physical location and proximity. Which of the following is the BEST solution for the pilot?

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

**Answer: A**

**Explanation:**

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

**NEW QUESTION 17**

- (Exam Topic 1)

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A reverse proxy
- B. A decryption certificate
- C. A split-tunnel VPN
- D. Load-balanced servers

**Answer: B**

**Explanation:**

A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.

To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

**NEW QUESTION 21**

- (Exam Topic 1)

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

- A. Security patches were uninstalled due to user impact.
- B. An adversary altered the vulnerability scan reports
- C. A zero-day vulnerability was used to exploit the web server
- D. The scan reported a false negative for the vulnerability

**Answer: A**

**Explanation:**

A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications.

If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.

The other options are not correct because:

> B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.

> C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.

> D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.

According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:

"A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers."

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

<https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/>

**NEW QUESTION 24**

- (Exam Topic 1)

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

- A. File integrity monitoring
- B. Honeynets
- C. Tcpreplay
- D. Data loss prevention

**Answer: D**

**Explanation:**

Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

**NEW QUESTION 29**

- (Exam Topic 1)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

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

**Answer: C**

**Explanation:**

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

### NEW QUESTION 30

- (Exam Topic 1)

When planning to build a virtual environment, an administrator need to achieve the following,

- Establish policies in Limit who can create new VMs
  - Allocate resources according to actual utilization'
  - Require justification 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. Protect 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 31

- (Exam Topic 1)

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

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

**Answer:** B

#### **Explanation:**

SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device<sup>1</sup>. SSH can encrypt both the authentication information and the data being exchanged between the client and the server<sup>2</sup>. SSH can be used to access and manage a NAS device remotely<sup>3</sup>.

### NEW QUESTION 35

- (Exam Topic 1)

Which of the following biometric authentication methods is the MOST accurate?

- A. Gait
- B. Retina
- C. Signature
- D. Voice

**Answer:** B

#### **Explanation:**

Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

### NEW QUESTION 40

- (Exam Topic 1)

Which of the following incident response steps occurs before containment?

- A. Eradication
- B. Recovery
- C. Lessons learned
- D. Identification

**Answer:** D

#### **Explanation:**

Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.

### NEW QUESTION 41

- (Exam Topic 1)

A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 10.0.0.1
```

Internet Address	Physical Address
10.10.255.255	ff-ff-ff-ff-ff-ff
10.0.0.1	aa-aa-aa-aa-aa-aa
10.0.0.254	aa-aa-aa-aa-aa-aa
224.0.0.2	01-00-5e-00-00-02

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

- A. Denial of service
- B. ARP poisoning
- C. Command injection
- D. MAC flooding

**Answer: B**

**Explanation:**

ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 6, page 271.

**NEW QUESTION 44**

- (Exam Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 47**

- (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 50**

- (Exam Topic 1)

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collision on the certificate key
- B. DNS hijacking to reroute traffic
- C. Brute force to the access point
- D. SSL/TLS downgrade

**Answer: B**

**Explanation:**

The attendee is experiencing delays in the connection, and the HTTPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.

Reference: <https://www.cloudflare.com/learning/dns/dns-hijacking/>

### NEW QUESTION 53

- (Exam Topic 1)

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

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

**Answer:** D

#### Explanation:

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

References:

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

### NEW QUESTION 54

- (Exam Topic 1)

While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

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

**Answer:** B

#### Explanation:

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

### NEW QUESTION 56

- (Exam Topic 1)

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 injection<sup>12</sup>. 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 applications<sup>34</sup>. 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 inspection<sup>34,45</sup>, 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 accordingly<sup>34</sup>.

### NEW QUESTION 58

- (Exam Topic 1)

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

- A. Vulnerabilities with a CVSS score greater than 6.9.
- B. Critical infrastructure vulnerabilities on non-IP protocols.
- C. CVEs related to non-Microsoft systems such as printers and switches.
- D. Missing patches for third-party software on Windows workstations and servers.

**Answer:** D

#### Explanation:

An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

### NEW QUESTION 62

- (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 65**

- (Exam Topic 1)

An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 66**

- (Exam Topic 1)

Which of the following roles would MOST likely have direct access to the senior management team?

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

**Answer:** C

**Explanation:**

A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders. A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.

The other options are not correct because:

- > A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
- > B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
- > D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:

“A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization.”

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://gdpr-info.eu/issues/data-protection-officer/>

**NEW QUESTION 69**

- (Exam Topic 1)

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

- A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities
- B. Install a sandbox to run the malicious payload in a safe environment
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

**Answer:** B

**Explanation:**

To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

**NEW QUESTION 72**

- (Exam Topic 1)

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user information between

nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

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

**Answer:** CD

**Explanation:**

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

**NEW QUESTION 75**

- (Exam Topic 1)

A security incident has been resolved. Which of the following BEST describes the importance of the final phase of the incident response plan?

- A. It examines and documents how well the team responded, discovers what caused the incident, and determines how the incident can be avoided in the future.
- B. It returns the affected systems back into production once systems have been fully patched, data restored, and vulnerabilities addressed.
- C. It identifies the incident and the scope of the breach, how it affects the production environment, and the ingress point.
- D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach.

**Answer:** A

**Explanation:**

The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 225.

**NEW QUESTION 78**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 80**

- (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 83**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can

help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. References: CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

#### NEW QUESTION 86

- (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 89

- (Exam Topic 2)

Which of the following can reduce vulnerabilities by avoiding code reuse?

- A. Memory management
- B. Stored procedures
- C. Normalization
- D. Code obfuscation

**Answer: A**

#### Explanation:

Memory management is a technique that can allocate and deallocate memory for applications and processes. Memory management can reduce vulnerabilities by avoiding code reuse, which is a technique that exploits a memory corruption vulnerability to execute malicious code that already exists in memory. Memory management can prevent code reuse by implementing features such as address space layout randomization (ASLR), data execution prevention (DEP), or stack canaries.

#### NEW QUESTION 94

- (Exam Topic 2)

A security investigation revealed that 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 following 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 99

- (Exam Topic 2)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 100

- (Exam Topic 2)

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).

- A. MAC filtering

- B. Zero trust segmentation
- C. Network access control
- D. Access control vestibules
- E. Guards
- F. Bollards.

**Answer:** AC

**Explanation:**

MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.

Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

**NEW QUESTION 102**

- (Exam Topic 2)

An organization wants to quickly assess how effectively the IT team hardened new laptops. Which of the following would be the best solution to perform this assessment?

- A. Install a SIEM tool and properly configure it to read the OS configuration files.
- B. Load current baselines into the existing vulnerability scanner.
- C. Maintain a risk register with each security control marked as compliant or non-compliant.
- D. Manually review the secure configuration guide checklists.

**Answer:** B

**Explanation:**

A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses. This is a quick and automated way to assess the hardening of the new laptops.

**NEW QUESTION 107**

- (Exam Topic 2)

A security administrator needs to provide secure access to internal networks for external partners. The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

- A. Kerberos
- B. SSL/TLS
- C. IPSec
- D. SSH

**Answer:** C

**Explanation:**

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References:  
<https://www.comptia.org/content/guides/what-is-vpn>

**NEW QUESTION 108**

- (Exam Topic 2)

Which of the following would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations?

- A. Machine learning
- B. DNS sinkhole
- C. Blocklist
- D. Honey pot

**Answer:** B

**Explanation:**

A DNS sinkhole would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations. A DNS sinkhole is a technique that involves redirecting malicious or unwanted domain names to an alternative IP address, such as a black hole, a honeypot, or a warning page. A DNS sinkhole can help to prevent or disrupt the communication between infected systems and command-and-control servers, malware distribution sites, phishing sites, or botnets. A DNS sinkhole can also help to identify and isolate infected systems by monitoring the traffic to the sinkhole IP address. References:

<https://www.comptia.org/blog/what-is-a-dns-sinkhole>

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

**NEW QUESTION 111**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 115**

- (Exam Topic 2)

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

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

**Answer:** B

**Explanation:**

Data is being exfiltrated when an internal system is sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Data exfiltration is the unauthorized transfer of data from a system or network to an external destination or actor. Data exfiltration can be performed by malicious insiders or external attackers who have compromised the system or network. DNS queries are requests for resolving domain names to IP addresses. DNS queries can be used as a covert channel for data exfiltration by encoding data in the domain names or subdomains and sending them to a malicious DNS server that can decode and collect the data. References:

<https://www.comptia.org/blog/what-is-data-exfiltration>

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

**NEW QUESTION 117**

- (Exam Topic 2)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

- A. MFA
- B. Lockout
- C. Time-based logins
- D. Password history

**Answer:** A

**Explanation:**

MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:

> <https://www.comptia.org/certifications/security>

> <https://www.youtube.com/watch?v=yCJyPPvM-xg>

> <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/>

**NEW QUESTION 118**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 123**

- (Exam Topic 2)

A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

- A. Change management procedure
- B. Information security policy
- C. Cybersecurity framework
- D. Secure configuration guide

**Answer:** D

**Explanation:**

A secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies. A security analyst can create baselines for the server team to follow when hardening new devices for deployment based on a secure configuration guide.

\* A. Change management procedure. This is not the correct answer, because a change management procedure is a document that describes the steps and processes for implementing, reviewing, and approving changes to an IT system or environment. A change management procedure helps to minimize the risks and impacts of changes on the system performance, availability, and security.

\* B. Information security policy. This is not the correct answer, because an information security policy is a document that defines the rules and principles for protecting the confidentiality, integrity, and availability of information assets within an organization. An information security policy helps to establish the roles and responsibilities of employees, managers, and stakeholders regarding information security.

\* C. Cybersecurity framework. This is not the correct answer, because a cybersecurity framework is a document that provides a set of standards, guidelines, and best practices for managing cybersecurity risks and improving resilience. A cybersecurity framework helps to align the business objectives and priorities with the security requirements and capabilities.

\* D. Secure configuration guide. This is the correct answer, because a secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies.

Reference: Secure Configuration Guide, Security Technical Implementation Guide - Wikipedia.

**NEW QUESTION 125**

- (Exam Topic 2)

Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 129**

- (Exam Topic 2)

A security team will be outsourcing several key functions to a third party and will require that:

- Several of the functions will carry an audit burden.
- Attestations will be performed several times a year.
- Reports will be generated on a monthly basis.

Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

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

**Answer:** C

**Explanation:**

A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom <https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968>

CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson <https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558>

Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

**NEW QUESTION 133**

- (Exam Topic 2)

Security analysts notice a server login from a user who has been on vacation for two weeks, The analysts confirm that the user did not log in to the system while on vacation After reviewing packet capture the analysts notice the following:

Which of the following occurred?

- A. A buffer overflow was exploited to gain unauthorized access.
- B. The user's account was compromised, and an attacker changed the login credentials.
- C. An attacker used a pass-the-hash attack to gain access.
- D. An insider threat with username logged in to the account.

**Answer:** C

**Explanation:**

A pass-the-hash attack is a type of replay attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is possible because some authentication protocols send hashes over the network instead of plain text passwords. The packet capture

shows that the attacker used NTLM authentication, which is vulnerable to pass-the-hash attacks

### NEW QUESTION 135

- (Exam Topic 2)

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

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

Which of the following password attacks is taking place?

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

**Answer: D**

#### Explanation:

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

### NEW QUESTION 136

- (Exam Topic 2)

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

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

**Answer: C**

#### Explanation:

A cloud access security broker (CASB) is a technology that can restrict access to internet services to authorized users only and control the actions each user can perform on each service. A CASB is a type of software or service that acts as an intermediary between users and cloud service providers. A CASB can enforce security policies, monitor user activity, detect and prevent data leaks, encrypt data, and provide visibility and auditability of cloud usage. References:

<https://www.comptia.org/blog/what-is-a-cloud-access-security-broker>

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

### NEW QUESTION 140

- (Exam Topic 2)

A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

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

**Answer: B**

#### Explanation:

Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.

References: 1

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2

CompTIA

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

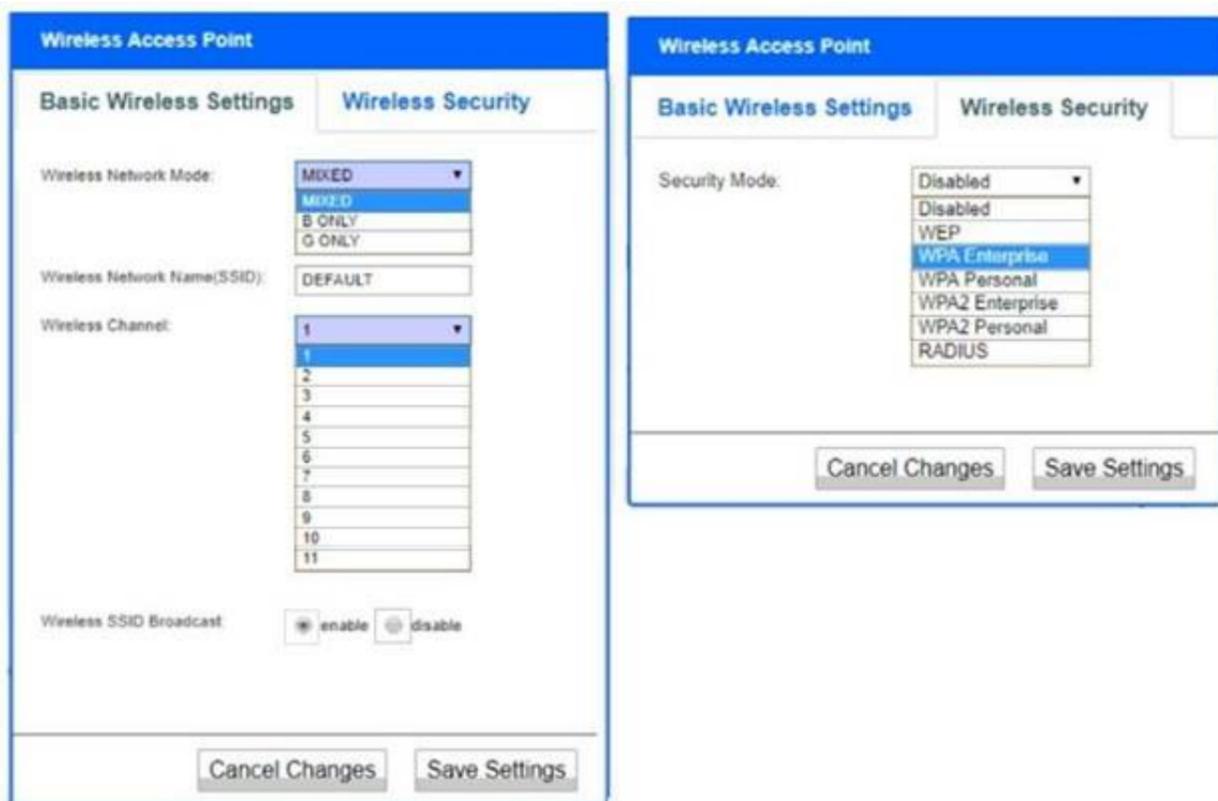
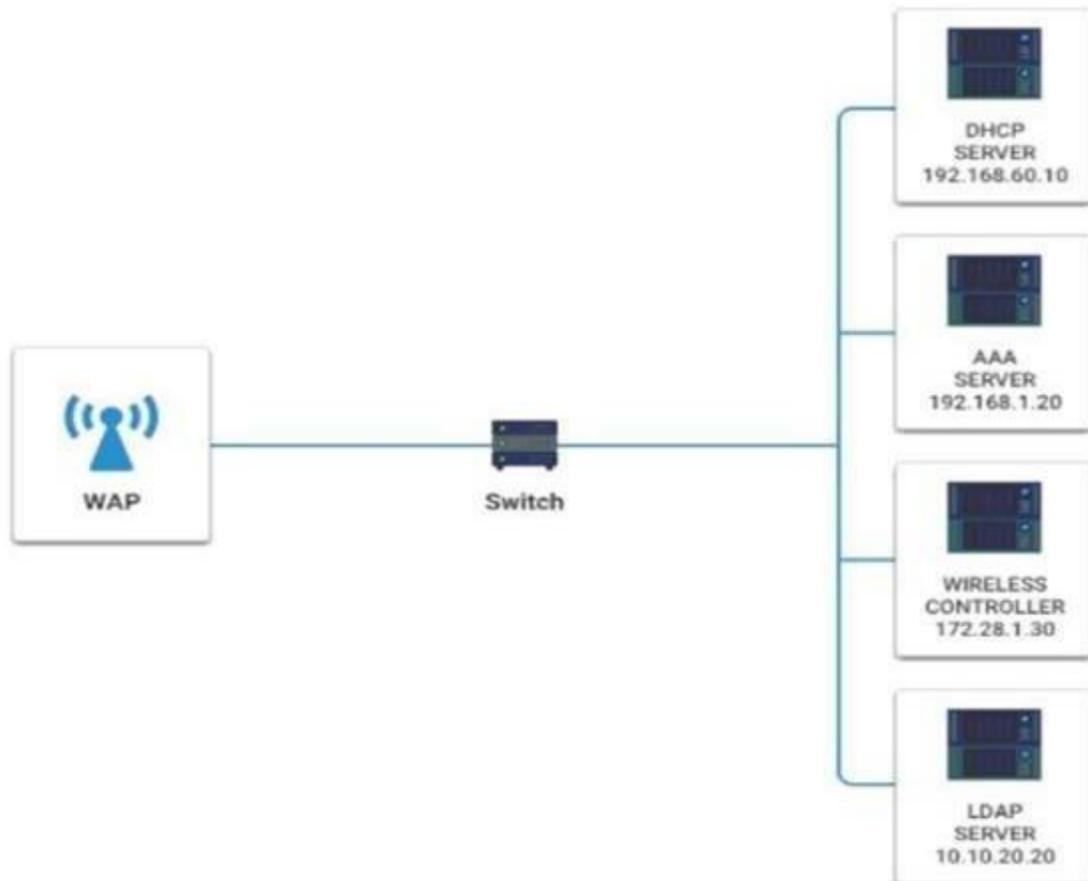
### NEW QUESTION 141

- (Exam Topic 2)

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS Please click on the below items on the network diagram and configure them accordingly:

- > WAP
- > DHCP Server
- > AAA Server
- > Wireless Controller
- > LDAP Server

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Wireless Access Point Network Mode – G only  
 Wireless Channel – 11  
 Wireless SSID Broadcast – disable  
 Security settings – WPA2 Professional

**NEW QUESTION 142**

- (Exam Topic 2)

A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:

- > Consistent power levels in case of brownouts or voltage spikes
- > A minimum of 30 minutes runtime following a power outage
- > Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

- A. Maintaining a standby, gas-powered generator
- B. Using large surge suppressors on computer equipment
- C. Configuring managed PDUs to monitor power levels

D. Deploying an appropriately sized, network-connected UPS device

**Answer:** D

**Explanation:**

A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

**NEW QUESTION 143**

- (Exam Topic 2)

Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

- A. Web metadata
- B. Bandwidth monitors
- C. System files
- D. Correlation dashboards

**Answer:** D

**Explanation:**

Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability. References:

<https://www.comptia.org/blog/what-is-a-correlation-dashboard>

**NEW QUESTION 144**

- (Exam Topic 2)

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

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

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 147**

- (Exam Topic 2)

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

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

Which of the following solutions would meet the requirements?

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

**Answer:** C

**Explanation:**

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources<sup>12</sup>. A PAM system can meet the requirements of the project by providing features such as:

- > Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin<sup>2</sup>g3.
- > The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on<sup>23</sup>. This prevents users from copying, changing, or sharing password<sup>2</sup>s.
- > Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as

frequency, complexity, and uniqueness<sup>23</sup>

. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise<sup>2</sup>.

> Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them<sup>23</sup>. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents<sup>2</sup>.

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner<sup>4</sup>. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.

A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification<sup>5</sup>. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login<sup>6</sup>. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

#### NEW QUESTION 151

- (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 152

- (Exam Topic 2)

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

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

**Answer: A**

#### Explanation:

Online Certificate Status Protocol (OCSP) is used to validate a certificate when it is presented to a user. OCSP is a protocol that allows a client or browser to query the status of a certificate from an OCSP responder, which is a server that maintains and provides the revocation status of certificates issued by a certificate authority (CA). OCSP can help to verify the authenticity and validity of a certificate and prevent the use of revoked or expired certificates. References:

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

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

#### NEW QUESTION 156

- (Exam Topic 2)

A security analyst is reviewing computer logs because a host was compromised by malware. After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

- A. Dump file
- B. System log
- C. Web application log
- D. Security tool

**Answer: A**

#### Explanation:

A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.

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

<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files>

#### NEW QUESTION 157

- (Exam Topic 2)

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work best to help identify potential vulnerabilities?

- A. hping3 -S comptia.org -p 80
- B. nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -sv
- D. nslookup -port 80 comptia.org

**Answer:** C

**Explanation:**

nmap is a network scanning tool that can perform various tasks such as port scanning, service detection, version detection, OS detection, vulnerability scanning, etc... nmap comptia.org -p 80 -sv is a command that scans port 80 (the default port for HTTP) on comptia.org domain name and tries to identify the service name and version running on that port. This can help identify potential vulnerabilities in the web server software by comparing the version with known exploits or patches.

**NEW QUESTION 161**

- (Exam Topic 2)

Several users have been violating corporate security policy by accessing inappropriate Sites on corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

- > Limit the sites that can be accessed
- > Only allow access to internal resources while physically on campus.
- > Restrict employees from downloading images from company email

Which of the following controls would best address this situation? (Select two).

- A. MFA
- B. GPS tagging
- C. Biometric authentication
- D. Content management
- E. Geofencing
- F. Screen lock and PIN requirements

**Answer:** DE

**Explanation:**

Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content<sup>1</sup>. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location<sup>2</sup>.

References:

- 1: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening>
- 2: <https://www.makeuseof.com/how-to-secure-your-content-management-system/>

**NEW QUESTION 166**

- (Exam Topic 2)

Which of the following threat actors is most likely to be motivated by ideology?

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

**Answer:** B

**Explanation:**

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

- > <https://www.uscybersecurity.net/hactivist/>
- > <https://www.fortinet.com/resources/cyberglossary/what-is-hactivism>

**NEW QUESTION 168**

- (Exam Topic 2)

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

- A. Salt string
- B. Private Key
- C. Password hash
- D. Cipher stream

**Answer:** C

**Explanation:**

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

- CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 2
- CompTIA Security+ Certification Exam Objectives, page 16, Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3

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

#### NEW QUESTION 169

- (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 174

- (Exam Topic 2)

A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

```
https://www.comptia.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was most likely observed?

- A. DLL injection
- B. Session replay
- C. SQLi
- D. xss

**Answer: D**

#### Explanation:

Cross-site scripting is a type of web application attack that involves injecting malicious code or scripts into a trusted website or application. The malicious code or script can execute in the browser of the victim who visits the website or application, and can perform actions such as stealing cookies, redirecting to malicious sites, displaying fake content, or compromising the system. References:

<https://www.comptia.org/blog/what-is-cross-site-scripting>

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

#### NEW QUESTION 178

- (Exam Topic 2)

A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommend?

- A. A content filter
- B. A WAF
- C. A next-generation firewall
- D. An IDS

**Answer: C**

#### Explanation:

A next-generation firewall (NGFW) is a solution that can defend against malicious actors misusing protocols and being allowed through network defenses. A NGFW is a type of firewall that can perform deep packet inspection, application-level filtering, intrusion prevention, malware detection, and identity-based access control. A NGFW can also use threat intelligence and behavioral analysis to identify and block malicious traffic based on protocols, signatures, or anomalies. References:

<https://www.comptia.org/blog/what-is-a-next-generation-firewall>

<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

#### NEW QUESTION 181

- (Exam Topic 2)

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

- A. Always-on
- B. Remote access
- C. Site-to-site
- D. Full tunnel

**Answer: C**

#### Explanation:

Site-to-site VPN is a type of VPN solution that connects two or more networks or sites across the public internet in a secure and encrypted way. Site-to-site VPN can be implemented using VPN appliances, such as firewalls or routers, that can establish and maintain the VPN tunnel between the sites. Site-to-site VPN can support multiple users or devices that need to access resources on the other site without requiring individual VPN clients or software. Site-to-site VPN is the best solution to support the new remote office, as it can provide secure and seamless connectivity between the office network and the main network of the organization.

Verified References:

- > Virtual Private Networks – SY0-601 CompTIA Security+ : 3.3 <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/virtual-private-networks-sy0-601-> (See Site-to-Site VPN)
- > VPN Technologies – CompTIA Security+ SY0-501 – 3.2 <https://www.professormesser.com/security-plus/sy0-501/vpn-technologies/> (See Site-to-Site VPN)
- > Security+ (Plus) Certification | CompTIA IT Certifications <https://www.comptia.org/certifications/security> (See Domain 3: Architecture and Design, Objective 3.3: Given a scenario, implement secure network architecture concepts.)

**NEW QUESTION 186**

- (Exam Topic 2)

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

A screenshot of a computer Description automatically generated with medium confidence

**NEW QUESTION 188**

- (Exam Topic 2)

An organization is repairing damage after an incident. Which Of the following controls is being implemented?

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

**Answer: C**

**Explanation:**

Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

**NEW QUESTION 190**

- (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 networks. 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 vulnerable.

### NEW QUESTION 193

- (Exam Topic 2)

A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?

- A. DLP
- B. SIEM
- C. NIDS
- D. WAF

**Answer: D**

#### Explanation:

WAF stands for Web Application Firewall, which is a type of firewall that can monitor, filter and block web traffic to and from web applications. WAF can protect web applications from common attacks such as cross-site scripting (XSS), SQL injection, directory traversal, buffer overflow and more. WAF can also enforce security policies and rules that can prevent parameter manipulation or tampering by an unknown third party. WAF is the best solution to help protect against the attack on the web API, as it can inspect the HTTP requests and responses and block any malicious or anomalous activity. Verified References:

> Other Application Attacks – SY0-601 CompTIA Security+ : 1.3 <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/other-application-attacks/> (See Web Application Firewall)

> CompTIA Security+ SY0-601 Exam Cram

<https://www.oreilly.com/library/view/comptia-security-sy0-601/9780136798767/ch03.xhtml> (See Web Application Firewall)

> Security+ domain #1: Attacks, threats, and vulnerabilities [updated 2021] <https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/> (See Web application firewall)

### NEW QUESTION 198

- (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 203

- (Exam Topic 2)

A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

- A. SIEM
- B. HIDS
- C. CASB
- D. EDR

**Answer: A**

#### Explanation:

SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

### NEW QUESTION 208

- (Exam Topic 2)

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account
- One of the websites the manager used recently experienced a data breach.
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.

Which of the following attacks has most likely been used to compromise the manager's corporate account?

- A. Remote access Trojan
- B. Brute-force
- C. Dictionary
- D. Credential stuffing
- E. Password spraying

**Answer:** D

**Explanation:**

Credential stuffing is a type of attack that involves using stolen or leaked usernames and passwords from one website or service to gain unauthorized access to other websites or services that use the same credentials. It can exploit the common practice of reusing passwords across multiple accounts. It is the most likely attack that has been used to compromise the manager's corporate account, given that the manager is using the same password across multiple external websites and the corporate account, and one of the websites recently experienced a data breach.

**NEW QUESTION 213**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 217**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 219**

- (Exam Topic 2)

Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?

- A. Shadow IT
- B. Hactivist
- C. Insider threat
- D. script kiddie

**Answer:** A

**Explanation:**

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge or approval of the IT or security group within the organization. Shadow IT can encompass cloud services, software, and hardware. The main area of concern today is the rapid adoption of cloud-based services.

According to one source, shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies.

**NEW QUESTION 221**

- (Exam Topic 2)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls
- C. NIST Risk Management Framework

D. ISO 27002

**Answer:** C

**Explanation:**

The NIST Risk Management Framework (RMF) is a process for evaluating the security of a system and implementing controls to reduce potential risks associated with it. The RMF process involves categorizing the system, selecting the controls that apply to the system, implementing the controls, and then assessing the success of the controls before authorizing the system. For more information on the NIST Risk Management Framework and other security processes, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

**NEW QUESTION 225**

- (Exam Topic 2)

A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

- A. Tape
- B. Full
- C. Image
- D. Snapshot

**Answer:** D

**Explanation:**

A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: <https://www.comptia.org/blog/what-is-a-snapshot-backup>

**NEW QUESTION 228**

- (Exam Topic 2)

Which of the following would be the best resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**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 can be the best resource for a software developer who is looking to improve secure coding practices for web applications by offering various tools, frameworks, standards, cheat sheets, testing guides, etc., that cover various aspects of web application security development and testing

**NEW QUESTION 231**

- (Exam Topic 2)

Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A. CVE
- B. CVSS
- C. CIA
- D. CERT

**Answer:** B

**Explanation:**

The correct answer is B. CVSS.

CVSS stands for Common Vulnerability Scoring System. It is a framework that provides a standardized way to measure the criticality of a vulnerability based on various factors, such as the impact, exploitability, and remediation level of the vulnerability. CVSS assigns a numerical score from 0 to 10 to each vulnerability, where 0 means no risk and 10 means the highest risk. CVSS also provides a qualitative rating for each score, such as low, medium, high, or critical. CVSS helps organizations prioritize the remediation of vulnerabilities based on their severity and potential impact<sup>12</sup>.

CVE stands for Common Vulnerabilities and Exposures. It is a list of publicly known and standardized identifiers for vulnerabilities and exposures in software and hardware systems. CVE provides a brief description of each vulnerability or exposure, but does not assign a score or rating to them. CVE helps organizations communicate and share information about vulnerabilities and exposures in a consistent and reliable way<sup>3</sup>.

CIA stands for Confidentiality, Integrity, and Availability. It is a model that defines the three main objectives of information security. Confidentiality means protecting data from unauthorized access or disclosure. Integrity means ensuring data is accurate and consistent and has not been tampered with. Availability means ensuring data is accessible and usable by authorized parties when needed. CIA helps organizations design and implement security controls and policies to protect their data and systems.

CERT stands for Computer Emergency Response Team. It is a group of experts who respond to security incidents and provide guidance and assistance to mitigate and prevent cyberattacks. CERT also conducts research and analysis on cybersecurity trends and issues, and disseminates information and best practices to the public. CERT helps organizations improve their security posture and resilience against cyber threats.

For more information on CVSS and other concepts related to vulnerability assessment and management, you can refer to [this video] or [this guide] from CompTIA Security+.

**NEW QUESTION 236**

- (Exam Topic 2)

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

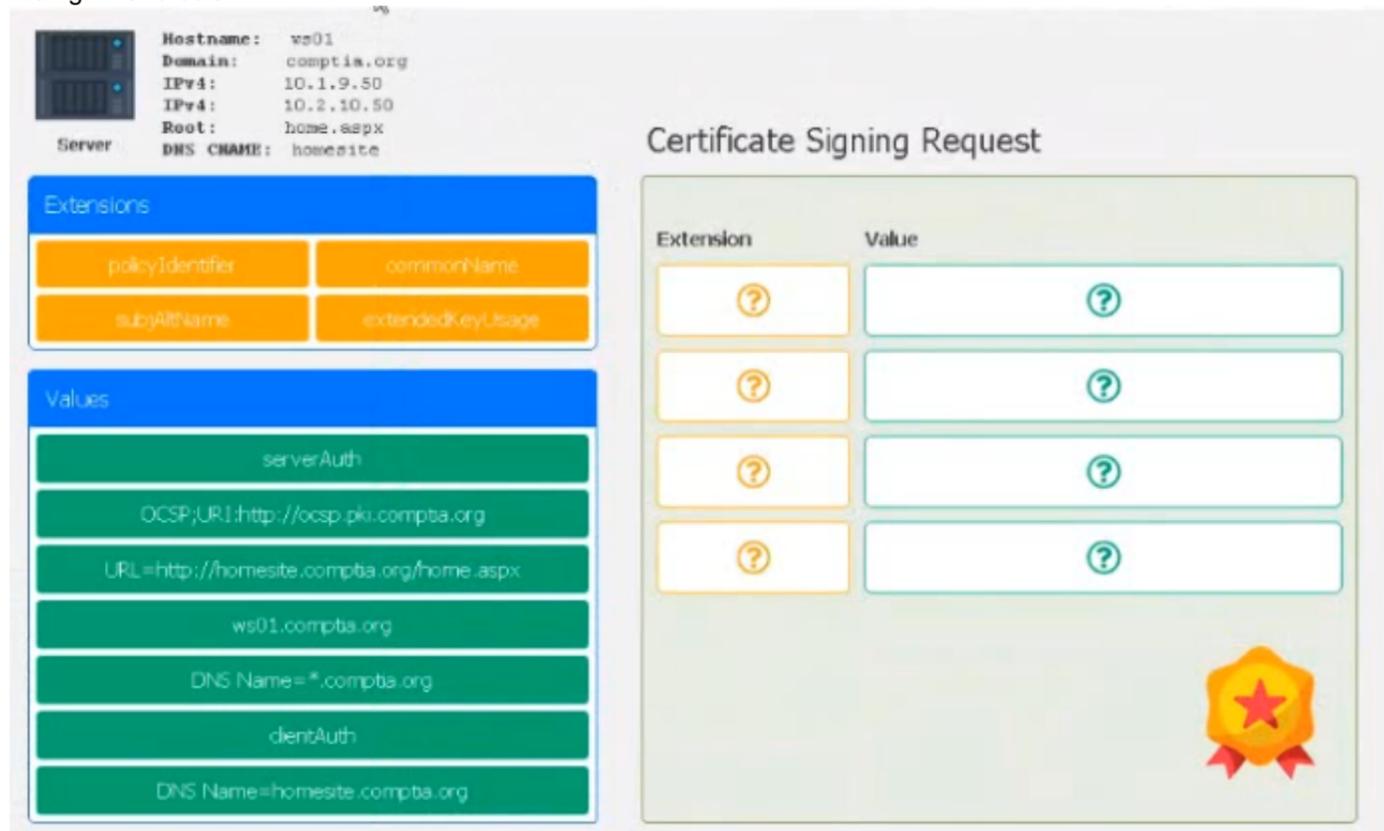
- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50

• IPv4: 10.2.10.50

• Root: home.aspx

• DNS CNAME: homesite. Instructions:

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

**NEW QUESTION 239**

- (Exam Topic 2)

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

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

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

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

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 244**

- (Exam Topic 2)

A security administrator needs to block a TCP connection using the corporate firewall, Because this connection is potentially a threat. the administrator not want to back an RST Which of the following actions in rule would work best?

- A. Drop
- B. Reject
- C. Log alert
- D. Permit

**Answer:** A

**Explanation:**

the difference between drop and reject in firewall is that the drop target sends nothing to the source, while the reject target sends a reject response to the source. This can affect how the source handles the connection attempt and how fast the port scanning is. In this context, a human might say that the best action to block a TCP connection using the corporate firewall is A. Drop, because it does not send back an RST packet and it may slow down the port scanning and protect against DoS attacks.

#### NEW QUESTION 247

- (Exam Topic 2)

While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements. Which of the following would be the BEST solution to securely prevent future issues?

- A. Using an administrator account to run the processes and disabling the account when it is not in use
- B. Implementing a shared account the team can use to run automated processes
- C. Configuring a service account to run the processes
- D. Removing the password complexity requirements for the user account

**Answer: C**

#### Explanation:

A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

#### NEW QUESTION 252

- (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 cleartext

**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.infosecrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/>

#### NEW QUESTION 255

- (Exam Topic 2)

A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?

- A. Recovery
- B. Lessons learned
- C. Containment
- D. Preparation

**Answer: C**

#### Explanation:

Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact. Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration

<https://www.fortinet.com/resources/cyberglossary/incident-response> <https://www.ibm.com/topics/incident-response>

#### NEW QUESTION 260

- (Exam Topic 2)

A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

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

**Answer: B**

#### Explanation:

Least privilege is a security principle that states that users and processes should only have the minimum level of access and permissions required to perform their tasks. This reduces the risk of insider threats by limiting the potential damage that a malicious or compromised user or process can cause to the system or data.

References: <https://www.comptia.org/blog/what-is-least-privilege>

#### NEW QUESTION 262

- (Exam Topic 2)

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at

the secondary subdomain level. Which of the following certificate properties will meet these requirements?

- A. HTTPS://\*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- C. HTTPS://\*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- D. HTTPS://".comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023

**Answer:** C

**Explanation:**

This certificate property will meet the requirements because it has a wildcard at the secondary subdomain level (.app1.comptia.org), which means it can be used for any subdomain under app1.comptia.org, such as test.app1.comptia.org or dev.app1.comptia.org. It also has a validity period of less than one year, which means it will need to be rotated annually. The other options do not meet the requirements because they either have a wildcard at the primary domain level (.comptia.org), which is not allowed, or they have a validity period of more than one year, which is too long.

**NEW QUESTION 264**

- (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 267**

- (Exam Topic 2)

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

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

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

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

**Answer:** D

**Explanation:**

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input<sup>1</sup>. A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system<sup>3</sup>.

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

John'; DROP TABLE users; -

This would result in the following SQL query being executed:

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

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

**NEW QUESTION 272**

- (Exam Topic 2)

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

- A. Soft token
- B. Smart card
- C. CSR

D. SSH key

**Answer:** D

**Explanation:**

SSH key is a pair of cryptographic keys that can be used for authentication and encryption when connecting to a remote Linux server via SSH protocol. SSH key authentication does not require a password and is more secure than password-based authentication. SSH key authentication also does not require additional software installation on the client or the server, as SSH is a built-in feature of most Linux distributions. A business partner can generate an SSH key pair on their own computer and send the public key to the company, who can then add it to the authorized\_keys file on the Linux server. This way, the business partner can access the Linux server without entering a password or installing any software

**NEW QUESTION 277**

- (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 282**

- (Exam Topic 2)

An organization decided not to put controls in place because of the high cost of implementing the controls compared to the cost of a potential fine. Which of the following risk management strategies is the organization following?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 284**

- (Exam Topic 2)

Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

- A. IP schema
- B. Application baseline configuration
- C. Standard naming convention policy
- D. Wireless LAN and network perimeter diagram

**Answer:** C

**Explanation:**

A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.

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/td/docs/solutions/Enterprise/Network\\_Virtualization/PathIsolationDesignGuide/P](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P)

**NEW QUESTION 285**

- (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, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

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

**Answer:** 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 286**

- (Exam Topic 2)

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

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

**Answer:** B

**Explanation:**

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

**NEW QUESTION 289**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system. A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users. References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.geeksforgeeks.org/rainbow-table-in-cryptography/>

**NEW QUESTION 291**

- (Exam Topic 2)

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

- A. Jamming
- B. BlueJacking
- C. Disassoaatm
- D. Evil twin

**Answer:** B

**Explanation:**

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

**NEW QUESTION 292**

- (Exam Topic 2)

Which of the following measures the average time that equipment will operate before it breaks?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 295**

- (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 298**

- (Exam Topic 2)

A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the following should be deployed first before allowing the use of personal devices to access company data?

- A. MDM
- B. RFID
- C. DLR
- D. SIEM

**Answer:** A

**Explanation:**

MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

**NEW QUESTION 303**

- (Exam Topic 2)

Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would best meet this need?

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

**Answer:** A

**Explanation:**

A community cloud deployment strategy would best meet the need of several universities participating in a collaborative research project and needing to share compute and storage resources. A community cloud is a type of cloud service model that provides a shared platform for multiple organizations with common interests, goals, or requirements. A community cloud can offer benefits such as cost savings, scalability, security, privacy, compliance, and collaboration.

References:

<https://www.comptia.org/blog/cloud-service-models-saas-paas-and-iaas-explained> <https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

**NEW QUESTION 307**

- (Exam Topic 2)

The most recent vulnerability scan flagged the domain controller with a critical vulnerability. The systems administrator researched the vulnerability and discovered the domain controller does not run the associated application with the vulnerability. Which of the following steps should the administrator take next?

- A. Ensure the scan engine is configured correctly.
- B. Apply a patch to the domain controller.
- C. Research the CVE.
- D. Document this as a false positive.

**Answer:** D

**Explanation:**

A false positive is a result that indicates a problem when there is no actual problem. In this case, the vulnerability scan flagged the domain controller with a critical vulnerability, but the domain controller does not run the application that is vulnerable. Therefore, the scan result is inaccurate and should be documented as a false positive.

\* A. Ensure the scan engine is configured correctly. This is not the next step, because the scan engine may be configured correctly and still produce false positives due to various factors, such as outdated signatures, network latency, or misconfigured devices.

\* B. Apply a patch to the domain controller. This is not the next step, because applying a patch to a system that does not have the vulnerability may cause unnecessary problems or conflicts.

\* C. Research the CVE. This is not the next step, because the systems administrator already researched the vulnerability and discovered that it does not affect the domain controller.

\* D. Document this as a false positive. This is the correct answer, because documenting false positives helps to improve the accuracy and efficiency of future scans and audits.

Reference: CompTIA Security+ Study Guide (PDF) - Netwrix, page 14.

**NEW QUESTION 309**

- (Exam Topic 2)

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

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

**Answer:** DF

**Explanation:**

A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.

To determine the sequence of a server farm's logs, the administrator should consider the following factors:

➤ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

➤ Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

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

**NEW QUESTION 310**

.....

## Relate Links

**100% Pass Your SY0-701 Exam with Examible Prep Materials**

<https://www.exambible.com/SY0-701-exam/>

## Contact us

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

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