SY0-601$^{\text{Q\&As}}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares. Which of the following should the company Implement?

A. DLP

B. CASB

C. HIDS

D. EDR

E. UEFI

Correct Answer: A

Chmod removes the setuido permission, that is, it removes the S bit. Setuido is the specific permission, but it is removed with Chmod.

https://www.cbtnuggets.com/blog/technology/system-admin/linux-file-permissions-understanding-setuid-setgid-and-the-sticky-bit

QUESTION 2

Which of the following describes the exploitation of an interactive process to gain access to restncted areas?

A. Persistence

B. Buffer overflow

C. Privilege escalation

D. Pharming

Correct Answer: C

https://en.wikipedia.org/wiki/Privilege_escalation#:~:text=Privilege%20escalation%20is%20the%20act,from%20an%20application%20or%20user

QUESTION 3

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing

B. Fuzzing

C. Manual code review

D. Dynamic code analysis

Correct Answer: D

Fuzzing: Injection of randomized data into a software program in an attempt to find system failures, memory leaks, error handling issues, and improper input validation

QUESTION 4

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

A. A captive portal

B. PSK

C. 802.1X

D. WPS

Correct Answer: C

Using a PKI for Wi-Fi authentication requires using the 802.1x standard for network access
https://www.securew2.com/blog/configuring-pki-wi-fi

QUESTION 5

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmapn

B. Heat maps

C. Network diagrams

D. Wireshark

Correct Answer: B

Heat maps directly correlate to wireless technology. A network diagram isn\\'t specific to wireless, and isn\\'t going to solve the issue.

QUESTION 6

Which of the following techniques eliminates the use of rainbow tables for password cracking?

A. Hashing

B. Tokenization

C. Asymmetric encryption

D. Salting

Correct Answer: D

Rainbow table attacks can easily be prevented by using salt techniques, which is a random data that is passed into the hash function along with the plain text.

QUESTION 7

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

Correct Answer: B

QUESTION 8

A security professional wants to enhance the protection of a critical environment that is used to store and manage a company\\'s encryption keys. The selected technology should be tamper resistant. Which of the following should the security professional implement to achieve the goal?

A. DLP

B. HSM

C. CA

D. FIM

Correct Answer: B

An HSM is a dedicated hardware device that provides a secure environment for cryptographic operations and key management. It is designed to be tamper-resistant, physically hardened, and provides strong protection for sensitive cryptographic material and keys. HSMs are often used in environments where secure and reliable key management is essential, such as in banking, financial institutions, or other critical systems where data confidentiality and integrity are paramount.

QUESTION 9

Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

A. Access control

B. Syslog

C. Session Initiation Protocol traffic logs

D. Application logs

Correct Answer: B

Since the threatening messages are reported to be voicemail messages, analyzing the Session Initiation Protocol (SIP) traffic logs would be the most appropriate action. SIP is a signaling protocol commonly used for initiating, maintaining, modifying, and terminating real-time communication sessions like voice and video calls over IP networks. Voicemail messages often involve SIP traffic, which includes information about the call setup and signaling details.

Analyzing SIP traffic logs can help the IT security team identify the source of the threatening voicemail messages, track the call flow, and gather information about the calling party. This can be crucial for understanding the nature of the threat and taking appropriate actions to mitigate or prevent further incidents.

QUESTION 10

Which of the following is the MOST relevant security check to be performed before embedding third-parry libraries in developed code?

A. Check to see if the third party has resources to create dedicated development and staging environments.

B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.

C. Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries\\' developers.

D. Read multiple penetration-testing reports for environments running software that reused the library.

Correct Answer: C

What to be done to best prevent issues in third-party code?

Establish a baseline and process for every third-party software that is introduced into the organisation, including performing a risk assessment to establish the risk associated with implementing a certain piece of code.

QUESTION 11

An organization has decided to host its web application and database in the cloud Which of the following BEST describes the security concerns for this decision?

A. Access to the organization\\'s servers could be exposed to other cloud-provider clients

B. The cloud vendor is a new attack vector within the supply chain

C. Outsourcing the code development adds risk to the cloud provider

D. Vendor support will cease when the hosting platforms reach EOL.

Correct Answer: B

QUESTION 12

Which of the following control types fixes a previously identified issue and mitigates a risk?

A. Detective

B. Corrective

C. Preventative

D. Finalized

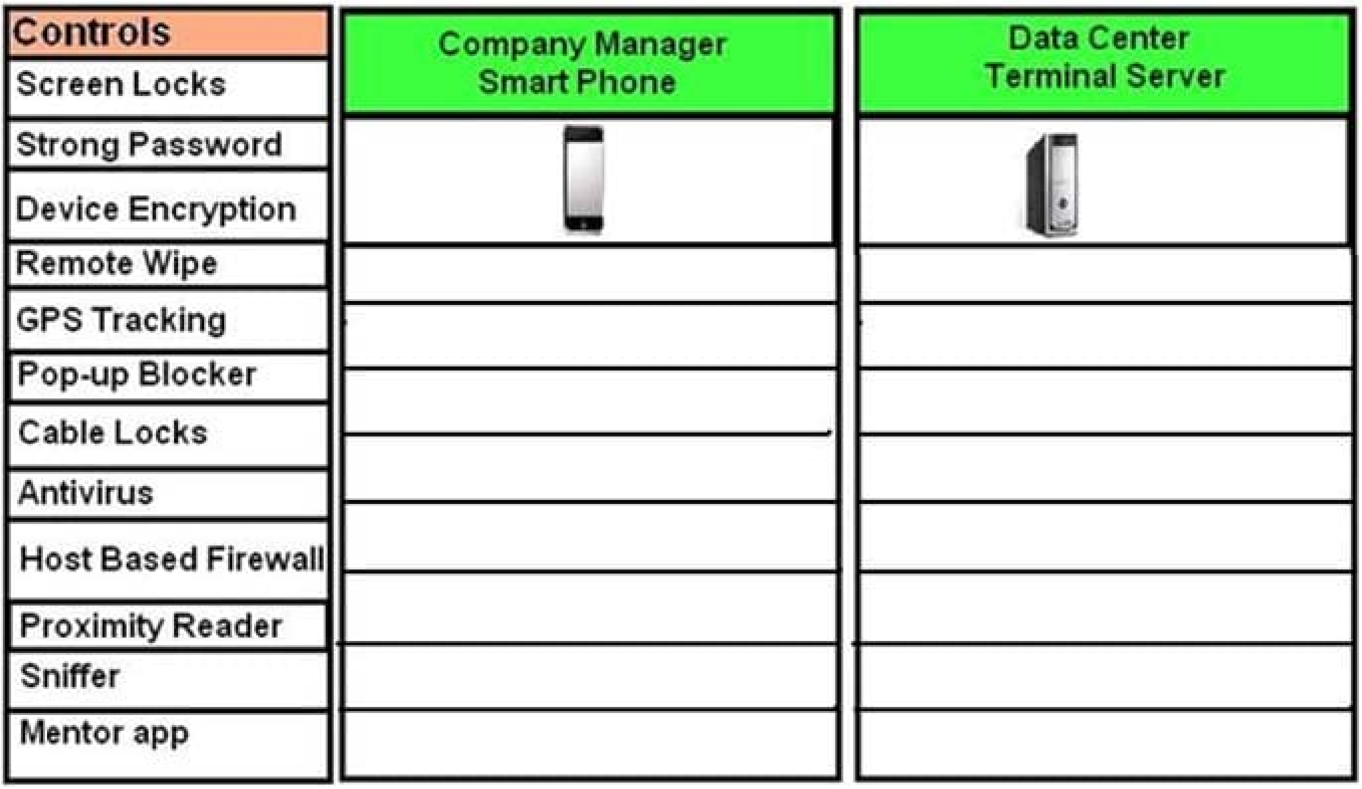
Correct Answer: B

QUESTION 13

DRAG DROP

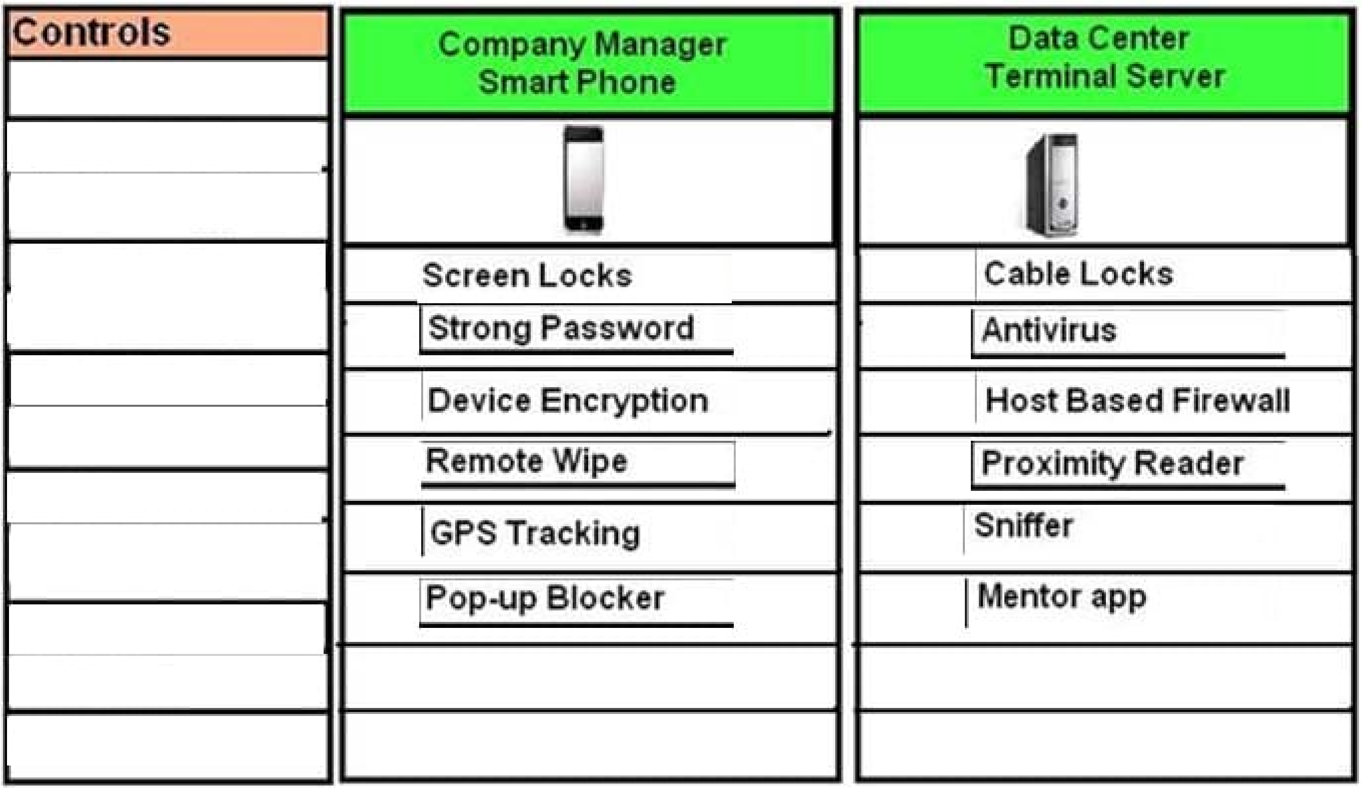
A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type. Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit.

Select and Place:



Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up Blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mentor app		

Correct Answer:



Controls	Company Manager Smart Phone	Data Center Terminal Server
	Screen Locks	Cable Locks
	Strong Password	Antivirus
	Device Encryption	Host Based Firewall
	Remote Wipe	Proximity Reader
	GPS Tracking	Sniffer
	Pop-up Blocker	Mentor app

Cable locks are used as a hardware lock mechanism

QUESTION 14

An organization is developing an authentication service for use at the entry and exit ports of country borders.

1.

The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports.

2.

The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time.

3.

The more frequently passengers travel, the more accurately the service will identify them.

Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice

B. Gait

C. Vein

D. Facial

E. Retina

F. Fingerprint

Correct Answer: BD

Most accurate according to the objectives

QUESTION 15

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

Correct Answer: D

A Web Application Firewall (WAF) is a security solution specifically designed to protect web applications and APIs from various attacks, including those that attempt to manipulate parameters and exploit vulnerabilities in the application layer. It sits between the clients (users or third parties) and the web server, inspecting the HTTP/HTTPS traffic and filtering out malicious requests.

In this scenario, the security analyst has identified that the web API is being abused by an unknown third party attempting to manipulate the parameters being passed to the API endpoint. A WAF would be able to analyze and validate the incoming requests to the API, blocking any requests that contain suspicious or malicious parameters. It can enforce security policies, perform input validation, and protect against common web application attacks like SQL injection, cross-site scripting (XSS), and parameter tampering.