SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

QUESTION 1

A security administrator would like to protect data on employees\\' laptops. Which of the following encryption techniques should the security administrator use?

A. Partition

B. Asymmetric

C. Full disk

D. Database

Correct Answer: C

Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive, including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or Trusted Platform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data. Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually. Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption. Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database.

References: Data Encryption -CompTIA Security+ SY0-401: 4.4, CompTIA Security+ Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course - Cybr, Application Hardening -SY0-601 CompTIA Security+ :

3.2.

QUESTION 2

A security analyst is assessing several company firewalls. Which of the following tools would the analyst most likely use to generate custom packets to use during the assessment?

A. hping

B. Wireshark

C. PowerShell

D. netstat

Correct Answer: A

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring

outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

QUESTION 3

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

A. Whaling

B. Credential harvesting

C. Prepending

D. Dumpster diving

Correct Answer: D

Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could

involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security

measures in cyber hygiene practices.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

QUESTION 4

Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement

B. Supply chain analysis

C. Right to audit clause

D. Due diligence

Correct Answer: A

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles

and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include

the following elements:

The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.

The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.

The testing team credentials and the authorized tools and techniques that they can use.

The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test. The status meeting and report schedules, formats, and recipients, as well as the confidentiality and nondisclosure agreements for the test results. The timeline and duration of the test, and the hours of operation and testing windows. The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage,

disruption, or disclosure of information. Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and

risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due

diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References: https://www.yeahhub.com/every-penetration-tester-you-should-know-about- this-rules-of-engagement/

https://bing.com/search?q=rules+of+engagement+penetration+testing

QUESTION 5

A company recently decided to allow employees to work remotely. The company wants to protect us data without using a VPN. Which of the following technologies should the company Implement?

A. Secure web gateway

B. Virtual private cloud end point

C. Deep packet Inspection

D. Next-gene ration firewall

Correct Answer: A

A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users\\' data

and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and remote access technologies.