SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

QUESTION 1

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX

B. CIRT

C. OSINT

D. TAXII

Correct Answer: D

Profess Messor notes:

Structured Threat Information eXpression (STIX)

?Describes cyber threat information

?Includes motivations, abilities, capabilities, and response information

Trusted Automated eXchange of Indicator Information (TAXII)

?Securely shares STIX data

Understand STIX/TAXII:

Structured Threat Information eXpression (STIX) is a standardized language and repetitional structure for the organization and dissemination of cyberthreat indicators and related information. Trusted Automated eXchange of Intelligence

Information (TAXII) is a standardized set of communication services, protocols, and message exchanges to support the effective communication and exchange of cyberthreat indicators.

QUESTION 2

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack

B. Protocol poisoning

C. Domain hijacking

D. Bluejacking

Correct Answer: A

On path attack is often known as man in the middle.

QUESTION 3

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

1.

Check-in/checkout of credentials

2.

The ability to use but not know the password

3.

Automated password changes

4.

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

Correct Answer: C

C. PAM via Messer Privileged access management (PAM) Managing superuser access

-Administrator and Root

-You don\\'t want this in the wrong hands Store privileged accounts in a digital vault

-Access is only granted from the vault by request

-These privileges are temporary PAM advantages

-Centralized password management

-Enables automation

-Manage access for each user

-Extensive tracking and auditin

QUESTION 4

Which of the following BEST describes the process of documenting who has access to evidence?

A. Order of volatility

B. Chain of custody

C. Non-repudiation

D. Admissibility

Correct Answer: B

QUESTION 5

A company is expanding its threat surface program and allowing individuals to security test the company\\'s internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A. Open-source intelligence

B. Bug bounty

C. Red team

D. Penetration testing

Correct Answer: B

Bug bounty programs are initiatives where organizations invite external security researchers or "white-hat" hackers to find and report security vulnerabilities in their systems. Researchers are rewarded with compensation based on the severity and impact of the discovered vulnerabilities.