312-85$^{\text{Q\&As}}$

Certified Threat Intelligence Analyst

QUESTION 1

Which of the following components refers to a node in the network that routes the traffic from a workstation to external command and control server and helps in identification of installed malware in the network?

A. Repeater

B. Gateway

C. Hub

D. Network interface card (NIC)

Correct Answer: B

QUESTION 2

Which of the following characteristics of APT refers to numerous attempts done by the attacker to gain entry to the target\\'s network?

A. Risk tolerance

B. Timeliness

C. Attack origination points

D. Multiphased

Correct Answer: C

QUESTION 3

Jian is a member of the security team at Trinity, Inc. He was conducting a real-time assessment of system activities in order to acquire threat intelligence feeds. He acquired feeds from sources like honeynets, P2P monitoring. infrastructure, and application logs.

Which of the following categories of threat intelligence feed was acquired by Jian?

A. Internal intelligence feeds

B. External intelligence feeds

C. CSV data feeds

D. Proactive surveillance feeds

Correct Answer: A

QUESTION 4

Moses, a threat intelligence analyst at InfoTec Inc., wants to find crucial information about the potential threats the organization is facing by using advanced Google search operators. He wants to identify whether any fake websites are hosted at the similar to the organization\\'s URL.

Which of the following Google search queries should Moses use?

A. related: www.infothech.org

B. info: www.infothech.org

C. link: www.infothech.org

D. cache: www.infothech.org

Correct Answer: A

QUESTION 5

Bob, a threat analyst, works in an organization named TechTop. He was asked to collect intelligence to fulfil the needs and requirements of the Red Tam present within the organization. Which of the following are the needs of a RedTeam?

A. Intelligence related to increased attacks targeting a particular software or operating system vulnerability

B. Intelligence on latest vulnerabilities, threat actors, and their tactics, techniques, and procedures (TTPs)

C. Intelligence extracted latest attacks analysis on similar organizations, which includes details about latest threats and TTPs

D. Intelligence that reveals risks related to various strategic business decisions

Correct Answer: B

QUESTION 6

John, a professional hacker, is trying to perform APT attack on the target organization network. He gains access to a single system of a target organization and tries to obtain administrative login credentials to gain further access to the systems in the network using various techniques.

What phase of the advanced persistent threat lifecycle is John currently in?

A. Initial intrusion

B. Search and exfiltration

C. Expansion

D. Persistence

Correct Answer: C

QUESTION 7

In which of the following storage architecture is the data stored in a localized system, server, or storage hardware and capable of storing a limited amount of data in its database and locally available for data usage?

A. Distributed storage

B. Object-based storage

C. Centralized storage

D. Cloud storage

Correct Answer: B

QUESTION 8

An analyst is conducting threat intelligence analysis in a client organization, and during the information gathering process, he gathered information from the publicly available sources and analyzed to obtain a rich useful form of intelligence. The information source that he used is primarily used for national security, law enforcement, and for collecting intelligence required for business or strategic decision making.

Which of the following sources of intelligence did the analyst use to collect information?

A. OPSEC

B. ISAC

C. OSINT

D. SIGINT

Correct Answer: C

QUESTION 9

In which of the following attacks does the attacker exploit vulnerabilities in a computer application before the software developer can release a patch for them?

A. Active online attack

B. Zero-day attack

C. Distributed network attack

D. Advanced persistent attack

Correct Answer: B

QUESTION 10

Sarah is a security operations center (SOC) analyst working at JW Williams and Sons organization based in Chicago. As a part of security operations, she contacts information providers (sharing partners) for gathering information such as collections of validated and prioritized threat indicators along with a detailed technical analysis of malware samples, botnets, DDoS attack methods, and various other malicious tools. She further used the collected information at the tactical and operational levels.

Sarah obtained the required information from which of the following types of sharing partner?

A. Providers of threat data feeds

B. Providers of threat indicators

C. Providers of comprehensive cyber-threat intelligence

D. Providers of threat actors

Correct Answer: C