Free Questions for CS0-002 by certscare

Shared by Burnett on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Image not found or type unknown

Which of the following describes what has occurred?

The host attempted to download an application from utoftor.com.

Options:

B) The host downloaded an application from utoftor.com.

C) The host attempted to make a secure connection to utoftor.com.

D) The host rejected the connection from utoftor.com.

Answer:

C

Explanation:

The packet capture shows that the host sent a Client Hello message to utoftor.com on port 443.This message is part of the TLS (Transport Layer Security) handshake protocol, which is used to establish a secure connection between a client and a server1. The Client Hello message contains information such as the supported TLS version, cipher suites, and extensions that the client can use for the secure connection. The server is expected to respond with a Server Hello message that selects the parameters for the secure connection. However, the packet capture does not show any response from the server, which means that the host only attempted to make a secure connection to utoftor.com, but did not succeed. The host did not download (B) or reject (D) any application from utoftor.com.

Question 2

Question Type: MultipleChoice

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.

Which of the following would be the MOST appropriate to remediate the controller?

Options:

A) Segment the network to constrain access to administrative interfaces.

B) Replace the equipment that has third-party support.

C) Remove the legacy hardware from the network.

D) Install an IDS on the network between the switch and the legacy equipment.

Answer:

A

Question 3

Question Type: MultipleChoice

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

Options:

A) Human resources

B) Public relations

C) Marketing

D) Internal network operations center

Answer:

B

Question 4

Question Type: MultipleChoice

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.

Which of the following would BEST identify potential indicators of compromise?

Options:

A) Use Burp Suite to capture packets to the SCADA device's IP.

B) Use tcpdump to capture packets from the SCADA device IP.

C) Use Wireshark to capture packets between SCADA devices and the management system.

D) Use Nmap to capture packets from the management system to the SCADA devices.

Answer:

C

Question 5

Question Type: **MultipleChoice**

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.

Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

Options:

A) FaaS

B) RTOS

C) SoC

D) GPS

E) CAN bus

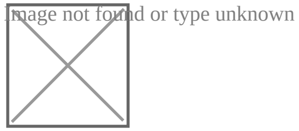
Answer:

E

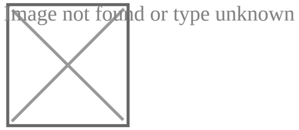
Question 6

Question Type: MultipleChoice

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:



The analyst runs the following command next:



Which of the following would explain the difference in results?

Options:

A) ICMP is being blocked by a firewall.

B) The routing tables for ping and hping3 were different.

C) The original ping command needed root permission to execute.

D) hping3 is returning a false positive.

Answer:

A

Question 7

Question Type: **MultipleChoice**

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.

Which of the following is the main concern a security analyst should have with this arrangement?

Options:

A) Making multiple trips between development sites increases the chance of physical damage to the FPGAs.

B) Moving the FPGAs between development sites will lessen the time that is available for security testing.

C) Development phases occurring at multiple sites may produce change management issues.

D) FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer:

C

Question 8

Question Type: **MultipleChoice**

A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.

Which of the following BEST describes this attack?

Options:

A) Injection attack

B) Memory corruption

C) Denial of service

D) Array attack

Answer:

C

Question 9

Question Type: MultipleChoice

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.

Which of the following should the analyst do FIRST?

Options:

A) Write detection logic.

B) Establish a hypothesis.

C) Profile the threat actors and activities.

D) Perform a process analysis.

Answer:

C

Question 10

Question Type: **MultipleChoice**

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server.

Which of the following is the FIRST step the analyst should take?

Options:

A) Create a full disk image of the server's hard drive to look for the file containing the malware.

B) Run a manual antivirus scan on the machine to look for known malicious software.

C) Take a memory snapshot of the machine to capture volatile information stored in memory.

D) Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer:

D