Free Questions for CCFH-202 by actualtestdumps

Shared by Rocha on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

Options:

A- Exploitation

B- Weaponization

C- Command & control

D- Installation

Answer:

B

Explanation:

Weaponization is the stage of the Cyber Kill Chain where the actor does not interact with the victim endpoint(s). Weaponization is where the actor prepares or packages the exploit or payload that will be used to compromise the target. This stage does not involve any communication or interaction with the victim endpoint(s), as it is done by the actor before delivering the weaponized content.

Exploitation, Command & Control, and Installation are all stages where the actor interacts with the victim endpoint(s), either by executing code, establishing communication, or installing malware.

Question 2

Question Type: MultipleChoice

In the MITRE ATT&CK Framework (version 11 - the newest version released in April 2022), which of the following pair of tactics is not in the Enterprise: Windows matrix?

Options:

A- Persistence and Execution

B- Impact and Collection

C- Privilege Escalation and Initial Access

D- Reconnaissance and Resource Development

Answer:

D

Explanation:

Reconnaissance and Resource Development are two tactics that are not in the Enterprise: Windows matrix of the MITRE ATT&CK Framework (version 11). These two tactics are part of the PRE-ATT&CK matrix, which covers the actions that adversaries take before compromising a target. The Enterprise: Windows matrix covers the actions that adversaries take after gaining initial access to a Windows system. Persistence, Execution, Impact, Collection, Privilege Escalation, and Initial Access are all tactics that are in the Enterprise: Windows matrix.

Question 3

Question Type: MultipleChoice

Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

Options:

A- MITRE ATT&CK

B- Lockheed Martin Cyber Kill Chain

C- Director of National Intelligence Cyber Threat Framework

D- NIST 800-171 Cyber Threat Framework

Answer:

A

Explanation:

MITRE ATT&CK is a threat framework that allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies. It is a knowledge base of adversary behaviors and tactics that covers various platforms, domains, and scenarios. It provides a common language and structure for threat hunters to understand and analyze threats, as well as to share findings and recommendations.

Question 4

Question Type: MultipleChoice

Which of the following is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain?

Options:

A- Installing a backdoor on the victim endpoint

B- Discovering internet-facing servers

C- Emailing the intended victim with a malware attachment

D- Loading a malicious payload into a common DLL

Answer:

B

Explanation:

Discovering internet-facing servers is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain. The RECONNAISSANCE phase is where the adversary researches and identifies targets, vulnerabilities, and attack vectors. Discovering internet-facing servers is a way for the adversary to find potential entry points or weaknesses in the target network.

Question 5

Question Type: MultipleChoice

Which tool allows a threat hunter to populate and colorize all known adversary techniques in a single view?

Options:

A- MISP

B- OWASP Threat Dragon

C- OpenXDR

D- MITRE ATT&CK Navigator

Answer:

D

Explanation:

MITRE ATT&CK Navigator is a tool that allows a threat hunter to populate and colorize all known adversary techniques in a single view. It is based on the MITRE ATT&CK framework, which is a knowledge base of adversary behaviors and tactics. The tool enables threat hunters to create custom matrices, layers, annotations, and filters to explore and model specific adversary techniques, with links to intelligence and case studies.

Question 6

Question Type: MultipleChoice

Lateral movement through a victim environment is an example of which stage of the Cyber Kill Chain?

Options:

A- Command & Control

B- Actions on Objectives

C- Exploitation

D- Delivery

Answer:

A

Explanation:

Lateral movement through a victim environment is an example of the Command & Control stage of the Cyber Kill Chain. The Cyber Kill Chain is a model that describes the phases of a cyber attack, from reconnaissance to actions on objectives. The Command & Control stage is where the adversary establishes and maintains communication with the compromised systems and moves laterally to expand

their access and control.