Free Questions for 200-201 by certsinside

Shared by Parks on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A user reports difficulties accessing certain external web pages. When an engineer examines traffic to and from the external domain in full packet captures, they notice that many SYNs have the same sequence number, source, and destination IP address, but they have different payloads. What is causing this situation?

Options:

A- TCP injection

B- misconfiguration of a web filter

C- Failure of the full packet capture solution

D- insufficient network resources

Answer:

A

Explanation:

TCP injection is an attack where the attacker sends crafted packets into an existing TCP session. These packets appear to be part of the session.

The presence of many SYN packets with the same sequence number, source, and destination IP but different payloads indicates that an attacker might be injecting packets into the session.

This method can be used to disrupt communication, inject malicious commands, or manipulate the data being transmitted.

Understanding TCP Injection Attacks

Analyzing Packet Captures for Injection Attacks

Network Security Monitoring Techniques

Question 2

Question Type: **MultipleChoice**

A member of the SOC team is checking the dashboard provided by the Cisco Firepower Manager for further Isolation actions. According to NIST SP800-61, in which phase of incident response is this action?

Options:

A- Cost-incident activity phase

B- Preparation phase

C- Selection and analyze phase

D- The radiation and recovery phase

Answer:

D

Explanation:

According to NIST SP800-61, the incident response lifecycle consists of four phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity.

When a SOC team member checks the Cisco Firepower Manager dashboard for further isolation actions, they are working within the Eradication and Recovery phase.

This phase focuses on removing the threat from the environment and recovering affected systems to normal operations.

NIST SP800-61 Computer Security Incident Handling Guide

Incident Response Phases Explained

Role of SOC in Incident Response

Question 3

Question Type: MultipleChoice

How is SQL injection prevented?

Options:

A- Address space layout randomization

B- Validate and sanitize user input

C- ...in the web server as a nonprivileged user

D- ...cost profiling

Answer:

B

Explanation:

SQL injection is a type of injection attack where malicious SQL statements are inserted into an entry field for execution.

The primary way to prevent SQL injection is by validating and sanitizing user input. This involves checking the input for malicious content and ensuring it adheres to expected patterns.

Prepared statements (parameterized queries) are also highly effective, as they treat user input as data rather than executable code.

Implementing these practices ensures that any input received from users does not manipulate SQL queries in a harmful way.

OWASP SQL Injection Prevention Cheat Sheet

Best Practices for Input Validation and Sanitization

Secure Coding Guidelines

Question 4

Question Type: **MultipleChoice**

Which statement describes indicators of attack?

Options:

A- internal hosts communicate with countries outside of the business range.

B- Phishing attempts on an organization are blocked by mall AV.

C- Critical patches are missing.

D- A malicious file is detected by the AV software.

Answer:

A

Explanation:

Indicators of Attack (IoA) refer to observable behaviors or artifacts that suggest a security breach or ongoing attack.

When internal hosts communicate with countries outside the business range, it may indicate data exfiltration or command-and-control communication to an external threat actor.

Unlike Indicators of Compromise (IoC) which indicate that a system has already been compromised, IoAs are often used to identify malicious activity in its early stages.

Monitoring for unusual outbound connections is a crucial aspect of detecting advanced persistent threats (APTs) and other sophisticated attacks.

Difference Between Indicators of Compromise and Indicators of Attack

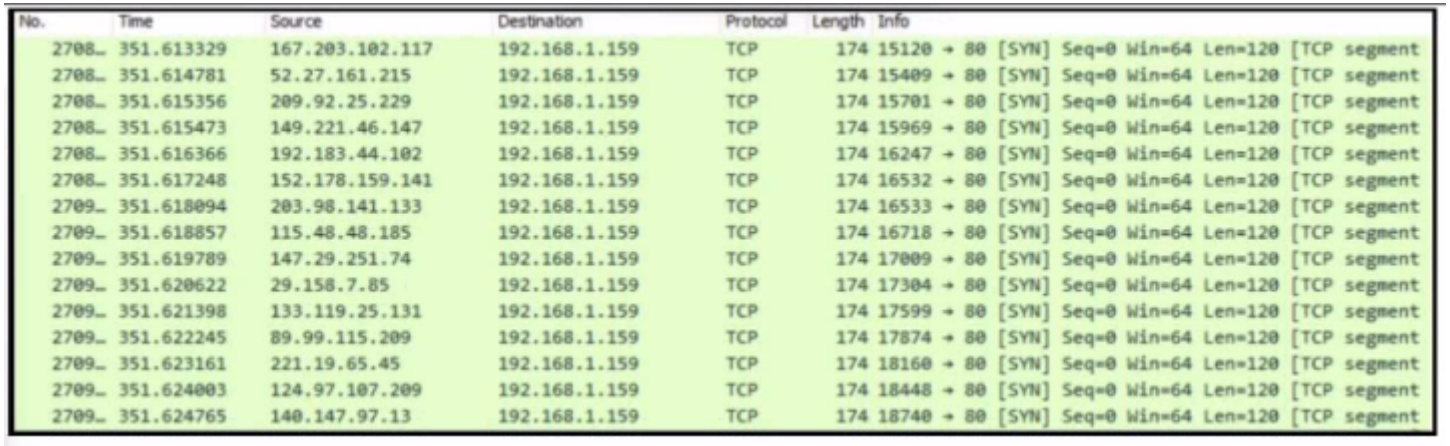
Cyber Threat Detection Using Indicators of Attack

Network Monitoring for Anomalous Behavior

Question 5

Question Type: **MultipleChoice**

Refer to exhibit.



No.	Time	Source	Destination	Protocol	Length	Info
2708…	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708…	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708…	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708…	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708…	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708…	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.623161	221.19.65.45	192.168.1.159	TCP	174	18160 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709…	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 → 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment

An engineer is Investigating an Intrusion and Is analyzing the pcap file. Which two key elements must an engineer consider? (Choose two.)

Options:

A- Variable 'info' field and unchanging sequence number

B- High volume oi SYN packets with very little variance in lime

C- identical length of 120 and window size (64)

D- SYN packets acknowledged from several source IP addresses

E- same source IP address with a destination port 80

Answer:

B, D

Explanation:

The exhibit shows a pcap file capturing multiple TCP SYN packets directed at the same destination IP address.

High volume of SYN packets with very little variance in time: This pattern is indicative of a SYN flood attack, a type of Denial of Service (DoS) attack where numerous SYN requests are sent to overwhelm the target system.

SYN packets acknowledged from several source IP addresses: This can be indicative of a Distributed Denial of Service (DDoS) attack where multiple compromised hosts (botnet) are used to generate traffic.

These characteristics suggest that the network is under a SYN flood or DDoS attack, aiming to exhaust the target's resources and disrupt service availability.

Understanding SYN Flood Attacks

Analysis of DDoS Attack Patterns

Wireshark Analysis Techniques for Intrusion Detection

Question 6

Question Type: **MultipleChoice**

How low does rule-based detection differ from behavioral detection?

Options:

A- Behavioral systems find sequences that match particular attach behaviors, and rule-based systems identify potential zero-day attacks.

B- Rule-based systems search for patterns linked to specific types of attacks, and behavioral systems Identify attacks per signature.

C- Behavioral systems have patterns are for complex environments, and rule-based systems can be used on low-mid-sized businesses.

D- Rule-based systems have predefined patterns, and behavioral systems learn the patterns that are specific to the environment.

Answer:

D

Explanation:

Rule-based detection systems operate using predefined patterns and signatures to identify known threats. These patterns are based on prior knowledge of attack methods and vulnerabilities.

Behavioral detection systems, on the other hand, analyze the normal behavior of a network or system to establish a baseline. They then monitor for deviations from this baseline, which may indicate potential threats.

Rule-based systems are effective at detecting known threats but may struggle with novel or zero-day attacks that do not match existing signatures.

Behavioral systems can detect unknown threats by recognizing abnormal activities, making them useful in identifying zero-day exploits and other sophisticated attacks.

Comparison of Rule-based and Behavioral Detection Methods in IDS

Advantages of Behavioral Analysis in Network Security

Cybersecurity Detection Techniques

Question 7

Question Type: MultipleChoice

Which of these is a defense-in-depth strategy principle?

Options:

A- identify the minimum resource required per employee.

B- Assign the least network privileges to segment network permissions.

C- Provide the minimum permissions needed to perform Job functions.

D- Disable administrative accounts to avoid unauthorized changes.

Answer:

C

Explanation:

Defense-in-depth is a layered security strategy that aims to protect information and resources through multiple security measures.

One of its key principles is the concept of least privilege, which means providing users and systems with the minimum level of access necessary to perform their job functions.

By assigning only the necessary permissions, the attack surface is reduced, and the potential damage from a compromised account or system is minimized.

This principle helps in mitigating the risk of unauthorized access and limits the capabilities of an attacker if they gain access to an account.

Defense-in-Depth Strategy by NIST

Principle of Least Privilege in Cybersecurity

Layered Security Approach Explained

Question 8

Question Type: **MultipleChoice**

Which type of attack uses a botnet to reflect requests off of an NTP server to overwhelm a target?

Options:

A- Display

B- Man-in-the-middle

C- Distributed denial of service

D- Denial of service

Answer:

C

Explanation:

A Distributed Denial of Service (DDoS) attack involves multiple compromised devices (botnet) sending a large number of requests to a target server to overwhelm it.

In a specific type of DDoS attack known as an NTP amplification attack, the attacker exploits the Network Time Protocol (NTP) servers by sending small queries with a spoofed source IP address (the target's IP).

The NTP server responds with a much larger reply to the target's IP address, thereby amplifying the traffic directed at the target.

This reflection and amplification technique significantly increases the volume of traffic sent to the target, causing denial of service.

OWASP DDoS Attack Overview

NTP Amplification Attack Explained

Understanding Botnets and Distributed Attacks

Question 9

Question Type: MultipleChoice

What is data encapsulation?

Options:

A- Browsing history is erased automatically with every session.

B- The protocol of the sending host adds additional data to the packet header.

C- Data is encrypted backwards, which makes it unusable.

D- Multiple hosts can be supported with only a few public IP addresses.

Answer:

B

Explanation:

Data encapsulation is a process in networking where the protocol stack of the sending host adds headers (and sometimes trailers) to the data.

Each layer of the OSI or TCP/IP model adds its own header to the data as it passes down the layers, preparing it for transmission over the network.

For example, in the TCP/IP model, data starts at the application layer and is encapsulated at each subsequent layer (Transport, Internet, and Network Access) before being transmitted.

This encapsulation ensures that the data is correctly formatted and routed to its destination, where the headers are stripped off in reverse order by the receiving host.

Networking Fundamentals by Cisco

OSI Model and Data Encapsulation Process

Understanding TCP/IP Encapsulation

Question 10

Question Type: **MultipleChoice**

A security engineer must investigate a recent breach within the organization. An engineer noticed that a breached workstation is trying to connect to the domain "Ranso4730-mware92-647". which is known as malicious. In which step of the Cyber Kill Chain is this event?

Options:

A- Vaporization

B- Delivery

C- reconnaissance

D- Action on objectives

Answer:

D

Explanation:

The event where a breached workstation is trying to connect to a known malicious domain suggests that the attacker is moving towards their end goals, which typically involves actions on objectives.

In the Cyber Kill Chain framework, 'Action on objectives' refers to the steps taken by an attacker to achieve their intended outcomes, such as data exfiltration, destruction, or ransom demands.

This phase involves the attacker executing their final mission within the target environment, leveraging access gained in earlier stages of the attack.

Lockheed Martin Cyber Kill Chain

Understanding the Stages of Cyber Attacks

Incident Response and the Cyber Kill Chain