KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **212-89**

Title : EC Council Certified Incident Handler (ECIH v2)

Version : DEMO

1.ZYX company experienced a DoS/DDoS attack on their network. Upon investigating the incident, they concluded that the attack is an application-layer attack.
Which of the following attacks did the attacker use?
A. Slowloris attack
B. UDP flood attack
C. SYN flood attack
D. Ping of ceath
Answer: A
Explanation:
The Slowloris attack is a type of application-layer attack that targets the web server by establishing and maintaining many simultaneous HTTP connections to the target server. Unlike traditional network-layer DoS/DDoS attacks such as UDP flood or SYN flood, Slowloris is designed to hold as many connections to the target web server open for as long as possible. It does so by sending partial requests, which are never completed, and periodically sending subsequent HTTP headers to keep the connections open. This consumes the server's resources, leading to denial of service as legitimate users cannot establish connections. The Slowloris attack is effective even against servers with a high bandwidth because it targets the server's connection pool, not its network bandwidth.
Reference: Incident Handler (ECIH v3) courses and study guides particularly emphasize understanding different types of attacks, including application-layer attacks like Slowloris, as part of the incident handling and response process.

2.Ross is an incident manager (IM) at an organization, and his team provides support to all users in the organization who are affected by threats or attacks. David, who is the organization's internal auditor, is also part of Ross's incident response team.
Which of the following is David's responsibility?
A. Configure information security controls.
B. Identify and report security loopholes to the management for necessary action.
C. Coordinate incident containment activities with the information security officer (ISO).
D. Perform the- necessary action to block the network traffic from the suspectoc intruder.
Answer: B
Explanation:
In the context of an incident response team, the role of an internal auditor like David includes identifying, evaluating, and reporting on information security risks and vulnerabilities within the organization. His responsibility is to ensure that the organization's security controls are effective and to identify any security loopholes that could be exploited by attackers. Once identified, he reports these vulnerabilities to management so that they can take the necessary actions to mitigate the risks. This role is critical in maintaining the organization’s overall security posture and ensuring compliance with relevant laws, regulations, and policies.
Reference: Incident Handler (ECIH v3) courses and study guides cover the roles and responsibilities of incident response team members, highlighting the importance of internal auditors in identifying and addressing security vulnerabilities.

3.Dash wants to perform a DoS attack over 256 target URLs simultaneously.
Which of the following tools can Dash employ to achieve his objective?

A. HOIC
B. IDAPro
C. Ollydbg
D. OpenVAS
Answer: A
Explanation:
High Orbit Ion Cannon (HOIC) is a tool designed to perform stress testing on networks or servers. It can launch a Distributed Denial of Service (DDoS) attack by enabling an attacker to overwhelm a target with HTTP POST and GET requests. HOIC's distinctive feature is its ability to attack multiple targets (up to 256 URLs simultaneously) with configurable HTTP flood attacks. This capability makes it a preferred choice for attackers aiming to disrupt services on a large scale. Unlike tools designed for debugging or vulnerability scanning (e.g., IDA Pro, Ollydbg, OpenVAS), HOIC is specifically crafted for launching DoS/DDoS attacks, making it the correct answer for Dash's objective.
Reference: The Incident Handler (ECIH v3) courses and study guides delve into various cyber attack tools, including HOIC, explaining their functionalities and potential impact as part of the comprehensive cybersecurity threat landscape education.

4.Which of the following information security personnel handles incidents from management and technical point of view?
A. Network administrators
B. Incident manager (IM)
C. Threat researchers
D. Forensic investigators
Answer: B
Explanation:
In the context of information security, the Incident Manager (IM) plays a crucial role in handling incidents from both a management and technical perspective. The Incident Manager is responsible for overseeing the entire incident response process, coordinating with relevant stakeholders, ensuring that incidents are analyzed, contained, and eradicated efficiently, and that recovery processes are initiated promptly. They are pivotal in ensuring communication flows smoothly between technical teams and upper management and that all actions taken are aligned with the organization's broader security policies and objectives. Unlike network administrators, threat researchers, or forensic investigators who may play more specialized roles within the incident response process, the Incident Manager has a broad oversight role that encompasses both technical and managerial aspects to ensure a comprehensive and coordinated response to security incidents.
Reference: Incident Handler (ECIH v3) courses and study guides emphasize the role of the Incident Manager as integral to the incident handling process, underscoring their importance in bridging the gap between technical response actions and strategic management decisions.

5.Francis received a spoof email asking for his bank information. He decided to use a tool to analyze the email headers.
Which of the following should he use?
A. EventLog Analyzer
B. MxToolbox

C. Email Checker
D. PoliteMail
Answer: B
Explanation:
MxToolbox is a comprehensive tool designed for analyzing email headers and diagnosing various email delivery issues. When Francis received a spoofed email asking for his bank information, using MxToolbox to analyze the email headers would be appropriate. This tool helps in examining the source of the email, tracking the email's path across the internet from the sender to the receiver, and identifying any signs of email spoofing or malicious activity. It provides detailed information about the email servers encountered along the way and can help in verifying the authenticity of the email sender. Other options like EventLog Analyzer, Email Checker, and PoliteMail are tools used for different purposes such as analyzing system event logs, checking email address validity, and managing email communications, respectively, and do not specifically focus on analyzing email headers to the extent required for investigating a spoofed email incident.
Reference: The use of MxToolbox in incident handling and email security analysis is commonly recommended in Incident Handler (ECIH v3) study materials as a practical tool for email header analysis and spoofing investigation.