ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: GIAC

Code: GCIH

Exam: GIAC Certified Incident Handler

https://www.examsnest.com/exam/gcih/

QUESTIONS & ANSWERS

DEMO VERSION

Question: 1

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:
Remove the network cable wires.
Isolate the system on a separate VLAN.
Use a firewall or access lists to prevent communication into or out of the system.
Change DNS entries to direct traffic away from compromised system.
Which of the following steps of the incident handling process includes the above actions?

A. Identification
B. Containment
C. Eradication
D. Recovery

Answer: B

Question: 2

Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.
Which of the following is the mostly likely the cause of the problem?

A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.

Answer: A

Question: 3

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack

C. Teardrop attack
D. Land attack

Answer: A

Question: 4

Which of the following types of attack can guess a hashed password?

A. Brute force attack
B. Evasion attack
C. Denial of Service attack
D. Teardrop attack

Answer: A

Question: 5

In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

A. Ping of death
B. Jolt
C. Fraggle
D. Teardrop

Answer: A

Question: 6

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.
Which of the following attacks has been occurred on the wireless network of Adam?

A. NAT spoofing
B. DNS cache poisoning
C. MAC spoofing
D. ARP spoofing

Answer: C

Question: 7

Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

A. Demon dialing
B. Warkitting
C. War driving
D. Wardialing

Answer: D

Question: 8

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses
B. Collecting employees information
C. Banner grabbing
D. Performing Neotracerouting

Answer: D

Question: 9

Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.

A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.

Answer: A, B, C

Question: 10

Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

A. Evasion attack
B. Denial-of-Service (DoS) attack

C. Ping of death attack
D. Buffer overflow attack

Answer: D

Thank You for trying the PDF Demo

Vendor: GIAC

Code: GCIH

Exam: GIAC Certified Incident Handler

https://www.examsnest.com/exam/gcih/