GCIH$^{\text{Q\&As}}$

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Which of the following services CANNOT be performed by the nmap utility? Each correct answer represents a complete solution. (Choose all that apply.)

A. Passive OS fingerprinting

B. Sniffing

C. Active OS fingerprinting

D. Port scanning

Correct Answer: AB

QUESTION 2

John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the We-are-secure server and alters its log files. Which of the following steps of malicious hacking includes altering the server log files?

A. Maintaining access

B. Covering tracks

C. Gaining access

D. Reconnaissance

Correct Answer: B

QUESTION 3

One type of FTP scan allows you to find a weakness in a certain type of firewall. These firewalls will allow an FTP data connection to take place, even though the FTP control connection hasn\\'t occurred. What is the root cause of this limitation?

A. The FTP server is not configured to require both the control connection and the data connection to pass inspection

B. The firewall is a sample packet-filtering firewall that is unable to recognize and test for existing connections

C. Because FTP control and data connections use the same port, the anomalous behavior should not be attributed to the firewall

D. The firewall has been kept patched and is therefore vulnerable to malicious scanning

Correct Answer: B

A simple packet-filtering firewall does not have the ability to recognize existing connections and will allow an FTP data connection, even if no control connection has taken place. Stateful firewalls do not share this limitation, since the control connection is recorded in the state table. On stateful firewalls, an incoming data connection is verified against the state table to check for an existing connection.

QUESTION 4

A successful phishing attack led to multiple user workstations being infected with command and control malware. Which of the following would be an effective short-term containment activity?

A. Search for hidden files and processes running on the hosts

B. Move hosts to a VLAN without Internet access

C. Block incoming port 80 and 443 traffic to the hosts

D. Deploy a web proxy to detect tunneled traffic

Correct Answer: B

Short-term containment is meant to stop the bleeding. Command and control traffic originates from compromised hosts and can be send via HTTP/HTTPS, DNS, and other protocols. Isolating a host on a private VLAN would be an effective response to stop C2 connections. C2 traffic is outbound not inbound, and most clients aren\\'t listening on ports 80/443. Root cause analysis and eradicating artifacts isn\\'t a short-term containment activity. A web proxy could be a longer term remediation identified in the lessons learned report or as part of recovery, but it would not be a containment activity.

QUESTION 5

FILL BLANK

Fill in the blank with the appropriate name of the rootkit.

A _______ rootkit uses device or platform firmware to create a persistent malware image.

A. firmware

Correct Answer: A