GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 2

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

QUESTION 3

Which of the following is a reason to implement security logging on a DNS server?

A. For preventing malware attacks on a DNS server

B. For measuring a DNS server\\'s performance

C. For monitoring unauthorized zone transfer

D. For recording the number of queries resolved

Correct Answer: C

QUESTION 4

What capability does a GRE tunnel provide to a bot herder communicating with his bots?

A. Encrypted payloads

B. Point-to-multipoint transmissions

C. VPN-like IP packet transfers

D. Stateful connections

Correct Answer: C

GRE tunnels are point-to-point, stateless, and enencrypted. They encapsulate and transfer packets from a source to a destination without the packets creating the tracks they would leave if they were sent outside the tunnel, obscuring where the packets originated.

QUESTION 5

An employee is sending personally threatening email through the company\\'s email server to a supervisor and external business partners. Which type of incident is this?

A. Phishing

B. Unauthorized use

C. Espionage

D. Intellectual property abuse

Correct Answer: B

Unauthorized use includes misuse of email in several ways, including abusive messages.