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

An incident handler investigating abnormal system behavior has captured traffic from two client workstations. Both clients sent dozens of SYN packets to an external host WW3.ACME.NET on port 80. In response, WW3.ACME.NET returned RST packets. When the incident handler browses to WW3.ACME.NET on port 80 from a workstation reserved for incident investigations, the traffic patterns do not match what is seen on the other two clients. Based on this information, what should the incident handler look for next?

A. Whether an IPS is identifying the outbound client traffic as malicious and blocking it.

B. Whether the external server is controlling infected hosts to map the internal network.

C. Whether the clients are infected and using crafted packets to transmit information.

D. Whether a firewall between the clients and external host is dropping packets.

Correct Answer: C

QUESTION 2

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Port scanning

B. ARP spoofing

C. Man-in-the-middle

D. Session hijacking

Correct Answer: B

QUESTION 3

Which of the following commands could a Windows administrator use to hardcode the MAC address for host 10.1.12.23 on his workstation?

A. netsh interface ip set address "Local Area Connection" static 10.1.12.23 255.255.255.0 10.1.12.1

B. ipconfig /renew

C. arp -s 10.1.12.23 8c:7b:9d:47:4e:dd

D. getmac /S 10.1.12.23 /u administrator

E. ifconfig eth0 inet 10.1.12.23 netmask 255.255.255.0

Correct Answer: C

The arp command can be used to display ARP entries as well as manipulate them. The getmac command is used to list

MAC addresses associated with each network card on a computer. The ipconfig command is used to display TCP/IP network configuration values and refresh DNS and DHCP settings. The netsh command displays and modifies network settings, such as IP address and netmask, but not the hardware address. The ifconfig command is a Linux/Unix command similar to Windows\\' ipconfig.

QUESTION 4

A security auditor is using John the Ripper to review password strength on Windows machines. The auditor knows that the company requires a 15-character minimum in their passwords. In this scenario, what format parameter must be passed to John (with Jumbo Patch) to crack the passwords?

A. --format=LANMAN

B. --format=UNIX

C. --format=NT

D. --format=SHA256

Correct Answer: D

QUESTION 5

What version of Windows natively supports SMB encryption?

A. Windows 8

B. Windows Server 2008

C. Windows 7

D. Windows Server 2003

Correct Answer: B

Reference: https://searchnetworking.techtarget.com/definition/Server-Message-Block-Protocol