# 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.pass4itsure.com/gcih.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

An attacker has used an infected USB thumb drive to compromise an internal host. The host is firewalled, blocking all inbound ports and protocols, and allowing tcp port 8080 outbound through an internal proxy. Which covert method would the attacker use to control the remote host?

A. Ptunnel

B. Passive FTP

C. Reverse HTTP shell

D. Covert_TCP

Correct Answer: C

A reverse HTTP shell allows an attacker to connect outbound over HTTP (regardless of port) and this will work through proxies as well. Ptunnel requires ICMP. Covert_TCP will not facilitate remote control. Passive FTP is not a covert method nor does it facilitate remote control.

**QUESTION 2**

One typical way to help secure applications such as Virtual Network Computing (VNC) is to send the application traffic using which of the following?

A. Secure Copy (SCP)

B. Secure Shell (SSH)

C. rlogin

D. IKE

Correct Answer: B

Secure Shell (SSH) is often used with other applications, such as VNC, in order to run the application through an encrypted tunnel and to protect the connection. SCP is used to securely copy files and cannot tunnel other applications. Rlogin does not encrypt data passed over the network.

**QUESTION 3**

You execute the following netcat command:

c:\target\nc -1 -p 53 -d -e cmd.exe

What action do you want to perform by issuing the above command?

A. Listen the incoming data and performing port scanning

B. Capture data on port 53 and performing banner grabbing

C. Capture data on port 53 and delete the remote shell

D. Listen the incoming traffic on port 53 and execute the remote shell

Correct Answer: D

**QUESTION 4**

FILL BLANK

Fill in the blank with the correct numeric value.

ARP poisoning is achieved in _____ steps.

A. 2

Correct Answer: A

**QUESTION 5**

Which of the following statements about reconnaissance is true?

A. It describes an attempt to transfer DNS zone data.

B. It is a computer that is used to attract potential intruders or attackers.

C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

D. It is also known as half-open scanning.

Correct Answer: A