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.geekcert.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

Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.

What is the name of this library?

A. PCAP

B. SysPCap

C. WinPCap

D. libpcap

Correct Answer: C

QUESTION 2

Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?

A. Kernel level rootkit

B. Boot loader rootkit

C. Hypervisor rootkit

D. Library rootkit

Correct Answer: C

QUESTION 3

Observe the following command; what is the analyst doing? $ rekal -f /cases/20160726_39/RAM/memimage.dd

A. Analyzing volatile evidence

B. Capturing a memory image

C. Verifying the integrity of an image

D. Creating a hash of original evidence

Correct Answer: A

The shown command starts the Rekall interpreter and invokes a memory image for analysis.

QUESTION 4

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Email spoofing

B. Steganography

C. Web ripping

D. Social engineering

Correct Answer: B

QUESTION 5

What is an effective mitigation for an HTTP flood attack?

A. Inspect connections using a reverse proxy and stall those showing repetitive patterns

B. Drop connections using the most bandwidth

C. Interrupt connections using CAPTCHA

D. Analyze requests and drop those using multiple GETs

Correct Answer: C

HTTP floods are difficult to mitigate through analysis of sessions or by statistical criteria because HTTP flood requests are designed to appear as normal traffic. Floods originate from bots that are running scripts that make normal-looking GET and POST requests in normal traffic volumes and with expected Useragent values. It is the collective bandwidth of all bots rather than high traffic from a single source that creates the DoS. Because they are bots that are running a script, they are unable to react to situations that require human interactions, like CAPTCHAs. Another characteristic of website traffic is its repetitiveness as users traverse pages in the site, which renders this ineffective as a tactic for preventing floods.