GCIA^{Q&As}

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

https://www.pass4itsure.com/gcia.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

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. Linux Live CD

B. DOS boot disk

C. Secure Authentication for EnCase (SAFE)

D. EnCase with a hardware write blocker

Correct Answer: C

QUESTION 2

You work as a Desktop Support Technician for umbrella Inc. The company uses a Windows-based network. An employee of the production department is facing the problem in the IP configuration of the network connection.

He called you to resolve the issue. You suspect that the IP configuration is not configured properly. You want to use the ping command to ensure that IPv4 protocol is working on a computer. While running the ping command from the

command prompt, you find that Windows Firewall is blocking the ping command. You enter the following command in the elevated command prompt on the computer:

netsh advfirewall firewall add rule name="ICMPv4" protocol=icmpv4:any,any dir=in action=allow

Which of the following actions will this command perform?

A. Permit ICMPv4 packet to pass through the firewall.

B. Permit ICMPv4 Echo Request.

C. Enable packet filtering by Windows Firewall.

D. Disable Firewall temporarily.

Correct Answer: A

QUESTION 3

Which of the following is an example of a social engineering attack?

A. Phishing

B. Man-in-the-middle attack

C. Browser Sniffing

D. E-mail bombing

Correct Answer: A

QUESTION 4

Which of the following switches is used with Pslist command on the command line to show the statistics for all active threads on the system, grouping these threads with their owning process?

A. Pslist -x

B. Pslist -m

C. Pslist -t

D. Pslist -d

Correct Answer: D

QUESTION 5

The promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it. Which of the following tools works by placing the host system network card into the promiscuous mode?

A. NetStumbler

B. Snort

C. THC-Scan

D. Sniffer

Correct Answer: D

[Latest GCIA Dumps](#) [GCIA VCE Dumps](#) [GCIA Exam Questions](#)