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.certbus.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 IPv4 to IPv6 transition methods uses encapsulation of IPv6 packets to traverse IPv4 networks?

A. Dual-stack

B. Translation

C. Tunneling

D. Stack

Correct Answer: C

QUESTION 2

Which of the following tools is used to analyze a system and report any unsigned drivers found?

A. regedit.exe

B. sigverify.exe

C. sigverif.exe

D. msconfig

Correct Answer: C

QUESTION 3

You work as a Network Administrator for a bank. For securing the bank\\'s network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network. After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed. What type of response is the IDS giving?

A. False Positive

B. True Negative

C. False Negative

D. True Positive

Correct Answer: C

QUESTION 4

Which of the following ICMP types refers to the message "Time Exceeded"?

A. Type 4

B. Type 12

C. Type 11

D. Type 5

Correct Answer: C

QUESTION 5

In which of the following attacks does a hacker imitate a DNS server and obtain the entire DNS database?

A. DNS poisoning attack

B. Illicit zone transfer attack

C. Illicit poisoning attack

D. DNS transfer attack

Correct Answer: B

QUESTION 6

Which of the following is used to provide a protective shield for the data passing over the Internet?

A. Proxy server

B. Intrusion detection system

C. Firewall

D. Tunneling

Correct Answer: D

QUESTION 7

What are the benefits of creating a new view using role-based CLI?

A. Scalability

B. Operational efficiency

C. Security

D. Availability

Correct Answer: BCD

QUESTION 8

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Fragmentation overlap attack

B. Evasion attack

C. Fragmentation overwrite attack

D. Insertion attack

Correct Answer: D

QUESTION 9

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?

A. FAU

B. FTK Imager

C. Galleta

D. Device Seizure

Correct Answer: D

QUESTION 10

Which of the following statements are true about an IPv6 network? Each correct answer represents a complete solution. Choose all that apply.

A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.

B. It increases the number of available IP addresses.

C. It provides improved authentication and security.

D. It uses 128-bit addresses.

E. It uses longer subnet masks than those used in IPv4.

Correct Answer: ABCD

QUESTION 11

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?

A. CHKDSK /I

B. CHKDSK /R /F

C. CHKDSK /C /L

D. CHKDSK /V /X

Correct Answer: B

QUESTION 12

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP-based network. You are configuring an Internet connection on a server. Which of the following servers filters outbound Web traffic on the network?

A. DHCP server

B. DNS server

C. Proxy server

D. WINS server

Correct Answer: C

QUESTION 13

Which of the following sectors on a hard disk contains codes that the computer uses to start the system?

A. Sector 256

B. Sector 0

C. Sector 1

D. Sector 128

Correct Answer: B

QUESTION 14

Which of the following are the two different file formats in which Microsoft Outlook saves e-mail messages based on system configuration? Each correct answer represents a complete solution. Choose two.

A. .txt

B. .pst

C. .xst

D. .ost

Correct Answer: BD

QUESTION 15

Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS X. He wants to boot his system from the Network Interface Controller (NIC). Which of the following snag keys will Mark use to perform the required function?

A. D

B. N

C. Z

D. C

Correct Answer: B