GCIA$^{\text{Q\&As}}$

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

QUESTION 1

You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an SSH terminal at home to connect to the company\\'s network. You have to configure your company\\'s router for it. By default, which of the following standard ports does the SSH protocol use for connection?

A. 80

B. 21

C. 443

D. 22

Correct Answer: D

QUESTION 2

Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?

A. Active IDS

B. Signature-based IDS

C. Passive IDS

D. Network-based IDS

Correct Answer: A

QUESTION 3

Which of the following ports is used for DNS services?

A. Port 7

B. Port 53

C. Port 80

D. Port 23

Correct Answer: B

QUESTION 4

For a host to have successful Internet communication, which of the following network protocols are required? You should assume that the users will not manually configure the computer in anyway and that the measure of success will be

whether the user can access Web sites after powering the computer and logging on.

Each correct answer represents a complete solution. Choose all that apply.

A. NTP

B. HTTP/HTTPS

C. DNS

D. DHCP

Correct Answer: BCD

QUESTION 5

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 6

Which of the following attacks involves multiple compromised systems to attack a single target?

A. Brute force attack

B. DDoS attack

C. Replay attack

D. Dictionary attack

Correct Answer: B

QUESTION 7

You work as a Network Administrator for Net Perfect Inc. The company\\'s network is configured with Internet Security and Acceleration (ISA) Server 2000 to provide firewall services. You want to block all e- mails coming from the domain named fun4you.com. How will you accomplish this?

A. Enable POP intrusion detection filterBlock e-mails from the fun4you.com domain

B. Enable SMTP filterAdd the fun4you.com domain name to the list of rejected domains

C. Create a site and content rule to prohibit access to the fun4you.com domain

D. Create a protocol rule that allows only authorized users to use the SMTP protocol

Correct Answer: B

QUESTION 8

Which of the following port numbers are valid ephemeral port numbers? Each correct answer represents a complete solution. Choose two.

A. 143

B. 1025

C. 161

D. 1080

Correct Answer: BD

QUESTION 9

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 10

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. Rainbow attack

B. DoS attack

C. ARP spoofing

D. Replay attack

Correct Answer: B

QUESTION 11

You work as a technician for Net Perfect Inc. You are troubleshooting a connectivity issue on a network. You are using the ping command to verify the connectivity between two hosts. You want ping to send larger sized packets than the usual 32-byte ones. Which of the following commands will you use?

A. ping -a

B. ping -4

C. ping -t

D. ping l

Correct Answer: D

QUESTION 12

Which of the following protocols uses only User Datagram Protocol (UDP)?

A. FTP

B. ICMP

C. TFTP

D. POP3

Correct Answer: C

QUESTION 13

Which of the following distributes incorrect IP address to divert the traffic?

A. IP spoofing

B. Domain name server (DNS) poisoning

C. Reverse Address Resolution Protocol

D. Route table poisoning

Correct Answer: B

QUESTION 14

What is the size of a subnet in IPv6?

A. 264 addresses

B. 232 addresses

C. 262 addresses

D. 2128 addresses

Correct Answer: A

QUESTION 15

Which of the following is computed from an arbitrary block of digital data for the purpose of detecting accidental errors?

A. Hash buster

B. Firewall

C. Checksum

D. Hash filter

Correct Answer: C