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.pass2lead.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

What is the order of the extension headers that is followed by IPv6?

A. Destination Options (first), Routing, IPv6 header, Hop-by-Hop, Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper-layer header, indicating payload.

B. Routing, Hop-by-Hop, Destination Options (first), Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper-layer header, indicating payload.

C. Fragment, Routing, Hop-by-Hop, Destination Options (first), Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper-layer header, indicating payload.

D. IPv6 header, Hop-by-Hop, Destination Options (first), Routing, Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper-layer header, indicating payload.

Correct Answer: D

QUESTION 2

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

A. It develops a new signature to find vulnerabilities.

B. It detects and alerts a computer user when it finds threats such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, well-known backdoors and system vulnerabilities, and DDoS clients.

C. It encrypts the log file using the 256 bit AES encryption scheme algorithm.

D. It is used as a passive trap to record the presence of traffic that should not be found on a network, such as NFS or Napster connections.

Correct Answer: ABD

QUESTION 3

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domain- based network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company\\'s security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that Windows firewall allows or blocks?

A. Configure Internet Protocol Security (IPSec).

B. Configure Network address translation (NAT).

C. Disable Windows firewall logging.

D. Enable Windows firewall logging.

Correct Answer: D

QUESTION 4

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 5

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 6

Which of the following commands will you use to display ARP packets in the snort-output?

A. snort -v -i eth 0

B. snort -d -v -i eth 0

C. snort -dev -i eth 0

D. snort -deva -i eth 0

Correct Answer: D

QUESTION 7

Which of the following statements about FTP is true?

A. It holds files transmitted through POP3 mail.

B. It manages network devices.

C. It connects file servers on the World Wide Web.

D. It transfers files between computers.

E. It allows password free file transfers.

Correct Answer: D

QUESTION 8

You are using a Windows-based sniffer named ASniffer to record the data traffic of a network. You have extracted the following IP Header information of a randomly chosen packet from the sniffer\\'s log:

45 00 00 28 00 00 40 00 29 06 43 CB D2 D3 82 5A 3B 5E AA 72

Which of the following TTL decimal values and protocols are being carried by the IP Header of this packet?

A. 41, UDP

B. 16, ICMP

C. 41, TCP

D. 16, UDP

Correct Answer: C

QUESTION 9

Which of the following information must the fragments carry for the destination host to reassemble them back to the original unfragmented state? Each correct answer represents a complete solution. Choose all that apply.

A. MF flag

B. Offset field

C. MAC address

D. Length of the data

E. IP address

F. IP identification number

Correct Answer: ABDF

QUESTION 10

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

A. War driving

B. Detecting unauthorized access points

C. Detecting causes of interference on a WLAN

D. WEP ICV error tracking

E. Making Graphs and Alarms on 802.11 Data, including Signal Strength

Correct Answer: D

QUESTION 11

You work as a Network Administrator for McNeil Inc. The company has a TCP/IP-based network. You are configuring an Internet connection for your company. Your Internet service provider (ISP) has a UNIX- based server. Which of the following utilities will enable you to access the UNIX server, using a text-based connection?

A. TELNET

B. IPCONFIG

C. PING

D. FTP

E. TRACERT

Correct Answer: A

QUESTION 12

At which port does a DHCPv6 client listen for DHCP messages?

A. TCP port 546

B. TCP port 547

C. UDP port 546

D. UDP port 547

Correct Answer: C

QUESTION 13

Which of the following protocols is used to translate IP addresses to Ethernet addresses?

A. Border Gateway Protocol (BGP)

B. Routing Information Protocol (RIP)

C. Address Resolution Protocol (ARP)

D. Internet Control Message Protocol (ICMP)

Correct Answer: C

QUESTION 14

Which of the following can be monitored by using the host-based intrusion detection system (HIDS)?

A. Computer performance

B. File system integrity

C. Computer storage space

D. DoS attack

Correct Answer: B

QUESTION 15

Which of the following firewalls keeps track of the state of network connections traveling across the network?

A. Stateful firewall

B. Application-level firewall

C. Packet filtering firewall

D. Circuit-level firewall

Correct Answer: A