GIAC

GSEC Exam

GIAC Security Essentials

[Questions & Answers Demo]

Version: 9.0

Question: 1

Which of the following are advantages of Network Intrusion Detection Systems (NIDS)?

A. Analysis of encrypted traffic
B. Provide insight into network traffic
C. Detection of network operations problems
D. Provide logs of network traffic that can be used as part of other security measures.
E. Inexpensive to manage

A. B, C, and D
B. A, C, and E
C. B, D, and E
D. A, B, and C

Answer: C

Explanation:

Question: 2

Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP
B. ARP
C. DNS
D. RDNS

Answer: A

Explanation:

Question: 3

What is the motivation behind SYN/FIN scanning?

A. The SYN/FIN combination is useful for signaling to certain Trojans.
B. SYN/FIN packets are commonly used to launch denial of service attacks against BSD hosts.
C. The crafted SYN/FIN packet sometimes gets past firewalls and filtering routers.
D. A SYN/FIN packet is used in session hijacking to take over a session.

Answer: B

Explanation:

Question: 4

There is not universal agreement on the names of the layers in the TCP/IP networking model. Which of the following is one of the functions of the bottom layer which is sometimes called the Network Access or Link Layer?

A. Provides end-to-end data delivery service for user applications
B. Handles the routing of the data packets over the network
C. Manages IP addressing and encryption for data packets
D. Defines the procedures for interfacing with Ethernet devices

Answer: D

Explanation:

Question: 5

Which of the following is a private, RFC 1918 compliant IP address that would be assigned to a DHCP scope on a private LAN?

A. 127.0.0.100
B. 169.254.1.50
C. 10.254.1.50
D. 172.35.1.100

Answer: C

Explanation: