



Vendor: GIAC

Exam Code: GSLC

Exam Name: GIAC Security Leadership

Version: DEMO

QUESTION NO: 1

Which of the following is used to describe the type of FTP access in which a user does not have permissions to list the contents of directories, but can access the contents if he knows the path and file name?

- A. Secure FTP
- B. Blind FTP
- C. Passive FTP
- D. Hidden FTP

Answer: B

QUESTION NO: 2

Which system is designed to analyze, detect, and report on security-related events?

- A. HIPS
- B. NIPS
- C. NIDS
- D. HIDS

Answer: B

QUESTION NO: 3

Which of the following viruses is designed to prevent antivirus researchers from examining its code by using various methods that make tracing and disassembling difficult?

- A. Armored virus
- B. Stealth virus
- C. Multipartite virus
- D. Polymorphic virus

Answer: A

QUESTION NO: 4

Which of the following provides security by implementing authentication and encryption on Wireless LAN (WLAN)?

- A. WEP
- B. WAP
- C. L2TP
- D. IPSec

Answer: A

QUESTION NO: 5

Which of the following are the examples of administrative controls?

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

- A. Security policy
- B. Auditing
- C. Security awareness training
- D. Data Backup

Answer: A,C

QUESTION NO: 6

John works as a Programmer for ABC Inc. On one of his routine visits to the company, he noted down the passwords of the employees while they were typing them on their computer screens.

Which of the following social engineering attacks did he just perform?

- A. Shoulder surfing
- B. Important user posing
- C. Dumpster diving
- D. Authorization by third party

Answer: A

QUESTION NO: 7

Which of the following encryption algorithms is applied in the PGP encryption system?

- A. TDE
- B. Triple DES
- C. Blowfish
- D. IDEA

Answer: D

QUESTION NO: 8

Rick, the Network Administrator of the ABC Inc., wants to design the initial test model for Internet Access. He wants to fulfill the following goals:

No external traffic should be allowed into the network.

Administrators should be able to restrict the websites which can be accessed by the internal users.

Which of the following technologies should he use to accomplish the above goals? (Click the Exhibit button on the toolbar to see the case study.)

- A. Internet Connection Sharing (ICS)
- B. Network Address Translator (NAT)
- C. Firewall

- D. Proxy Server
- E. Routing and Remote Access Service (RRAS)

Answer: D

QUESTION NO: 9

You work as a Network Administrator for ABC Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The domain functional level is set to Windows Server 2003. You have configured an Active Directory-integrated DNS zone on the network. A new security policy dictates that each incoming DNS query should be recorded. Which of the following steps will you take to implement the new security policy?

A. Create a GPO.

Configure Audit Object Access.

Attach the GPO to the domain.

B. Do nothing, each incoming DNS queries is recorded by default in DNS.LOG file.

C. Enable debug logging on the DNS server.

D. Create a new OU.

Move the DNS server account to the OU.

Create a GPO.

Configure Audit Logon events.

Attach the GPO to the OU.

Answer: C

QUESTION NO: 10

Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

A. Identifying the risk

B. Finding an economic balance between the impact of the risk and the cost of the countermeasure

C. Identifying the accused

D. Assessing the impact of potential threats

Answer: A,B,D