GIAC

Exam GSLC

GIAC Security Leadership Certification (GSLC)

Version: 6.0

[Total Questions: 567]

Topic 1, Volume A

Question No : 1 - (Topic 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 - (Topic 1)

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 - (Topic 1)

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 - (Topic 1)

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 - (Topic 1)

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 - (Topic 1)

John works as a Programmer for We-are-secure 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 - (Topic 1)

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 - (Topic 1)

Rick, the Network Administrator of the Fimbry Hardware 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 - (Topic 1)

You work as a Network Administrator for Net Perfect 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 - (Topic 1)

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

Question No : 11 - (Topic 1)

The promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it. Which of the following tools works by placing the host system network card into the promiscuous mode?

A. Sniffer

B. THC-Scan
C. NetStumbler
D. Snort

Answer: A

Question No : 12 - (Topic 1)

Janet is the project manager of the NHQ Project for her company. Janet is nearly done leading the project and there have been no cost or schedule overruns in the development of the new software for her company. The project team has been completing their work on time and there is still $75,000 left in the project budget. Janet decides to have the project team implement some extra features to the project scope to use all of the $75,000 in the budget even though the customer didn't specifically ask for the added features. This scenario is an example of which one of the following?

A. Scope creep
B. Gold plating
C. Change management
D. Value added change

Answer: B

Question No : 13 - (Topic 1)

You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

A. Automated penetration testing
B. Code review
C. Manual penetration testing
D. Vulnerability scanning

Answer: D

Question No : 14 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate word.

A_____ is a computer system on the Internet that is expressly set up to attract and trap people who attempt to penetrate other people's computer systems.

Answer: honeypot

Question No : 15 - (Topic 1)

Which of the following protocols is used as a transport protocol for Internet dial-up connections?

A. SMTP
B. SNMP
C. DHCP
D. PPP

Answer: D

Question No : 16 - (Topic 1)

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2008. The company's headquarters is located at Los Angeles. A branch office of the company is located at Denver. You are about to send a message to Rick who is a Network Administrator at Denver. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys will you use to encrypt the message?

A. Your public key
B. The recipient's private key
C. The recipient's public key
D. Your private key

Answer: C

Question No : 17 - (Topic 1)

Which of the following programs can collect various types of personal information, such as Internet surfing habits, and Web sites that the user has visited?

A. Spyware
B. Honeypot
C. Worm
D. Malware

Answer: A

Question No : 18 - (Topic 1)

Which of the following applications would be considered a data warehousing application?

A. Golf score tracking
B. Badge reader
C. Fraud detection
D. eCommerce site

Answer: C

Question No : 19 - (Topic 1)

Which of the following options is an approach to restricting system access to authorized users?

A. MIC
B. MAC
C. RBAC
D. DAC

Answer: C

Question No : 20 - (Topic 1)

Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP

Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company's security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company's security policy. What will he do to accomplish this?

Each correct answer represents a part of the solution. Choose three.

A. Configure the authentication type for the wireless LAN to Open system.
B. Install a firewall software on each wireless access point.
C. Configure the authentication type for the wireless LAN to Shared Key.
D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
E. Broadcast SSID to connect to the access point (AP).
F. On each client computer, add the SSID for the wireless LAN as the preferred network.

Answer: C,D,F

Question No : 21 - (Topic 1)

You are the project manager for your organization and are trying to determine which vendor your organization will use. You have determined that any vendor that would like to bid on your project work will need to have a Microsoft Certified System Engineer on staff, have eight years of Cisco experience, and have at least two references from similar projects. What have you created in this scenario?

A. Screening system for the vendors
B. Weighting system for the vendors
C. Preferred vendors list
D. Bidders conference

Answer: A

Question No : 22 - (Topic 1)

Which of the following tools is based on Linux and used to carry out the Penetration Testing?

A. JPlag

B. BackTrack
C. Vedit
D. Ettercap

Answer: B

Question No : 23 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate type of router.

A _____ router performs packet-filtering and is used as a firewall.

Answer: screening

Question No : 24 - (Topic 1)

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He wants to test the response of a DDoS attack on the we-are-secure server. To accomplish this, he takes the following steps:

Instead of directly attacking the target computer, he first identifies a less secure network named Infosecure that contains a network of 100 computers.

He breaks this less secure network and takes control of all its computers. After completing this step, he installs a DDoS attack tool on each computer of the Infosecure network.

Finally, he uses all the computers of the less secure network to carry out the DDoS attack on the we-are-secure server.

Which of the following tools can John use to accomplish the task?

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

A. Stacheldraht
B. Trin00
C. TFN
D. BackOfficer Friendly

Answer: A,B,C