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.leads4pass.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

With reference to the given case study, one of the security goals requires to configure a secure connection between the Boston distribution center and the headquarters. You want to implement IP filter to fulfill the security requirements. How should you implement IP filters at the headquarters? (Click the Exhibit button on the toolbar to see the case study.)

A. Add source filters for the headquarters for UDP port 80 and IP protocol 50.Add destination filters for the Boston distribution center for UDP port 80 and IP protocol 50.

B. Add source filters for the Boston distribution center for UDP port 80 and IP protocol 50.Add destination filters for headquarters for UDP port 80 and IP protocol 50.

C. Add source filters for the Boston distribution center for UDP port 1701 and IP protocol 50.Add destination filters for the headquarters for UDP port 1701 and IP protocol 50.

D. Add source filters for the headquarters for UDP port 1701 and IP protocol 50.Add destination filters for the Boston distribution center for UDP port 1701 and IP protocol 50.

Correct Answer: C

QUESTION 2

Which of the following Windows XP system files handles memory management, I/O operations, and interrupts?

A. Ntoskrnl.exe

B. Advapi32.dll

C. Kernel32.dll

D. Win32k.sys

Correct Answer: C

QUESTION 3

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft\\'s Windows XP operating system?

A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

B. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe

C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

D. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe

Correct Answer: D

QUESTION 4

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. Linux Live CD

B. DOS boot disk

C. Secure Authentication for EnCase (SAFE)

D. EnCase with a hardware write blocker

Correct Answer: C

QUESTION 5

Which of the following hacking tools provides shell access over ICMP?

A. John the Ripper

B. Loki

C. Nessus

D. Nmap

Correct Answer: B

QUESTION 6

Which of the following commands displays the IPX routing table entries?

A. sh ipx traffic

B. sh ipx route

C. sh ipx int e0

D. sho ipx servers

Correct Answer: B

QUESTION 7

Which of the following forensic tool suite is developed for Linux operating system?

A. Wetstone

B. MForensicsLab

C. ProDiscover

D. S.M.A.R.T.

Correct Answer: D

QUESTION 8

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

A. False accusations

B. False victimization

C. Encouraging others to harass the victim

D. Attempts to gather information about the victim

Correct Answer: A

QUESTION 9

You work as a Network Administrator for McNeil Inc. The company\\'s Windows 2000-based network is configured with Internet Security and Acceleration (ISA) Server 2000. You configure intrusion detection on the server. Which of the following alerts notifies that repeated attempts to a destination computer are being made and no corresponding ACK (acknowledge) packet is being communicated?

A. IP half scan attack

B. UDP bomb attack

C. Land attack

D. Ping of death attack

Correct Answer: A

QUESTION 10

Fill in the blank with the appropriate facts regarding IP version 6 (IPv6).

IP addressing version 6 uses_____ -bit address. Its____ IP address assigned to a single host allows the host to send and receive data.

A. IP addressing version 6 uses 128 -bit address. Its unicast IP address assigned to a single host allows the host to send and receive data.

Correct Answer: A

QUESTION 11

Which of the following tools is used to locate lost files and partitions to restore data from a formatted, damaged, or lost partition in Windows and Apple Macintosh computers?

A. Easy-Undelete

B. VirtualLab

C. File Scavenger

D. Recover4all Professional

Correct Answer: B

QUESTION 12

Rick works as the Network Administrator of Baby Blue Inc. He wants to upgrade the existing network to the Active Directory based Windows 2000 network. He configures a DNS on the network. Which of the following is the primary reason that the DNS is required in an Active Directory environment?

A. Without installing the DNS, you cannot install the Active Directory in the network.

B. Netlogon uses the DNS to find a domain controller in the network.

C. The Active Directory uses the DNS zone transfer protocol during replication.

D. The Active Directory is stored within the DNS database.

Correct Answer: B

QUESTION 13

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. Stunnel

B. IPTables

C. IPChains

D. OpenSSH

Correct Answer: B

QUESTION 14

Which of the following types of Intrusion detection systems (IDS) is used for port mirroring?

A. Port address-based IDS

B. Network-based IDS (NIDS)

C. Host-based IDS (HIDS)

D. Anomaly-based IDS

Correct Answer: B

QUESTION 15

Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Tunneling proxy server

B. Reverse proxy server

C. Anonymous proxy server

D. Intercepting proxy server

Correct Answer: D