Vendor: GIAC

Exam Code: GCIA

Exam Name: GIAC Certified Intrusion Analyst

Version: DEMO

QUESTION 1
You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Enable verbose logging on the firewall
B. Install a network-based IDS
C. Install a DMZ firewall
D. Install a host-based IDS

Answer: B

QUESTION 2
Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files
B. EDB and STM database files
C. Temporary files
D. cookie files

Answer: ABC

QUESTION 3
Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover. Which of the following Steganography methods is Victor using to accomplish the task?

A. The distortion technique
B. The spread spectrum technique
C. The cover generation technique
D. The substitution technique

Answer: A

QUESTION 4
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple smallsized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Nessus
B. Y.A.T.
C. Whisker
D. Fragroute

Answer: AC

QUESTION 5
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You want to know the current TCP/IP network configuration settings, DHCP server IP address, and DHCP lease expiration date of your network.

Which of the following utilities will you use?

A. PING
B. TELNET
C. TRACERT
D. IPCONFIG

Answer: D

QUESTION 6
You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are connected to a switch device. One day, users complain that they are unable to connect to a file server. You try to ping the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.

What is the most likely cause?

A. The switch device is not working.
B. The cable that connects the server to the switch is broken.
C. Automatic IP addressing is not working.
D. The server's NIC is not working.
E. The server is configured with unspecified IP address.

Answer: D

QUESTION 7
John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. Rainbow attack
B. DoS attack
C. ARP spoofing
D. Replay attack

Answer: B

QUESTION 8
John works as a Network Security Administrator for NetPerfect Inc. The manager of the company

has told John that the company's phone bill has increased drastically. John suspects that the company's phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. War dialing
B. Sequence++ attack
C. Phreaking
D. Man-in-the-middle attack

Answer: C

QUESTION 9
You are implementing a host based intrusion detection system on your web server. You feel that the best way to monitor the web server is to find your baseline of activity (connections, traffic, etc.) and to monitor for conditions above that baseline. This type of IDS is called _____.

A. Anomaly Based
B. Reactive IDS
C. Passive IDS
D. Signature Based

Answer: A

QUESTION 10
Which of the following is the default port for POP3?

A. 21
B. 110
C. 80
D. 25

Answer: B

QUESTION 11
You work as a network administrator for BlueWell Inc. You have to convert your 48-bit host address (MAC address) to an IPv6 54-bit address. Using the IEEE-EUI-64 conversion process, how do you convert the 48-bit host address (MAC address) to an IPv6 54-bit address?

A. Add EF. FE between the third and fourth bytes.
B. Add FE. EE between the third and fourth bytes.
C. Add FF. EE between the third and fourth bytes.
D. Add FF. FE between the third and fourth bytes

Answer: D

QUESTION 12
Which of the following units of data does the data-link layer send from the network layer to the physical layer of the OSI model?

A. Protocols
B. Raw bits
C. Data packets
D. Data frames
E. Data segments

Answer: D

QUESTION 13
The following output is generated by running the show ip route command:

```
RouterA#show ip route

< - - Output Omitted for brevity - ->
```

```
Gateway of last resort is 172.18.1.1 to network 0.0.0.0

    192.168.0.0/24 is subnetted, 2 subnets
R      192.168.11.0 [120/1] via 172.18.50.1, 00:00:00, Serial0/0
R      192.168.12.0 [120/1] via 172.18.60.1, 00:00:00, Serial0/1
C      192.168.10.0/24 is directly connected, FastEthernet0/0
C      192.168.20.0/24 is directly connected, FastEthernet0/1
R*  0.0.0.0/0 [120/1] via 172.18.1.1, 00:00:17, Serial2/0
```

Which next hop address will RouterA use in forwarding traffic to 10.10.100.0/24?

A. 172.18.50.1
B. 192.168.10.0
C. 172.18.1.1
D. 172.18.60.1

Answer: C

QUESTION 14
Which of the following types of firewall ensures that the packets are part of the established session?

A. Switch-level firewall
B. Application-level firewall
C. Stateful inspection firewall
D. Circuit-level firewall

Answer: C

QUESTION 15
Which of the following terms describes an attempt to transfer DNS zone data?

A. Reconnaissance

B. Encapsulation
C. Dumpster diving
D. Spam

Answer: A

QUESTION 16
You work as a Network Administrator for McRobert Inc. Your company has a TCP/IP-based network. You want to get the protocol statistics and the active TCP/IP network connections of your computer. Which of the following will you use?

A. IPSTAT
B. SNMP
C. ARP
D. NBTSTAT
E. NETSTAT

Answer: E

QUESTION 17
What are the limitations of the POP3 protocol?

Each correct answer represents a complete solution. Choose three.

A. E-mails can be retrieved only from the Inbox folder of a mailbox. E-mails stored in any other folder are not accessible.
B. It is only a retrieval protocol. It is designed to work with other applications that provide the ability to send e-mails.
C. It does not support retrieval of encrypted e-mails.
D. It uses less memory space.

Answer: ABC

QUESTION 18
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.

Answer: D

QUESTION 19
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.

Answer: D

QUESTION 20
Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

Each correct answer represents a part of the solution. Choose all that apply.

A. Text Semagrams
B. Linguistic steganography
C. Technical steganography
D. Perceptual masking

Answer: AB

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**