DUMPSBOSS.COM

SCNP Strategic Infrastructure Security

Exin SCNP

Version Demo

Total Demo Questions: 15

Total Premium Questions: 244

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	101
Topic 2, Volume B	143
Total	244

QUESTION NO: 1

Which three of the following are examples of the reason that Message Authentication is needed?

A. Packet Loss

B. Content Modification

C. Masquerading

D. Public Key Registration

E. Sequence Modification

ANSWER: B C E

QUESTION NO: 2

Which of the following pieces of information are found in the Inode, on a Linux system?

A. Directory Location

B. File ownership information

C. File size in Bytes

D. Filename

E. File access time

ANSWER: B C E

QUESTION NO: 3

The test.doc file on your Linux system that needs the ownership changed. You wish to have the new owner of the file to be vp_finance. Which of the following is the command to change ownership to the

vp_finance user account?

A. ch_own vp_finance test_doc

B. chown vp_finance test.doc

C. chown test/doc vp_finance

D. chown vp_finance test/doc

E. ch_own vp_finance test.doc

ANSWER: B

QUESTION NO: 4

You have just become the senior security professional in your office. After you have taken a complete inventory of the network and resources, you begin to work on planning for a successful security implementation in the network. You are aware of the many tools provided for securing Windows 2003 machines in your network. What is the function of The

Security Configuration and Analysis snap-in?

A. This tool is used to manage the NTFS security permissions on objects in the domain.

B. This tool is used to create an initial security database for the domain.

C. This tool is used to analyze a large number of computers in a domain-based infrastructure.

D. This tool provides an analysis of the local system security configuration.

E. This tool provides a single point of management where security options can be applied to a local computer or can be imported to a GPO.

ANSWER: D

QUESTION NO: 5

You have become the lead security professional for a mid-sized organization. You are currently studying DNS issues, and configuration options. You come across the concepts of

DNS Spoofing, and investigate more. What is DNS Spoofing?

A. DNS Spoofing is when the DNS client submits a false DNS request to the DNS server, and the DNS server responds with correct data.

B. DNS Spoofing is the DNS client submits a DNS request to the DNS server using a bogus IP address, and the DNS server responds to the incorrect host.

C. DNS Spoofing is when a DNS Server responds to an unauthorized DNS client, providing that client with name resolution.

D. DNS Spoofing is when a DNS client is forced to make a DNS query to an imposter DNS server, which send the client to an imposter resource.

E. DNS spoofing is when a DNS server provides name resolution to clients that are located in a different IP subnet than the server itself.

ANSWER: D

QUESTION NO: 6

As you configure your SuSe Linux computer, you make sure to modify TCP Wrappers as required by the security policy. What are two benefits that TCP Wrappers provides you with in controlling the security of the system?

A. Connection Logging

B. Password Encryption

C. Network Encryption

D. Network Access Control

E. Secure Packet Encapsulation

ANSWER: A D

QUESTION NO: 7

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```
                                                              _|□|x|
File  Edit  Format  Help
10/28-18:05:45.378701 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:1 TCP TTL:57 TOS:0x0 ID:62554 IpLen:20 DgmLen:40
******S* Seq: 0x2A9F61BD  Ack: 0x0  Win: 0x800  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-18:05:45.422227 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:2 TCP TTL:57 TOS:0x0 ID:34117 IpLen:20 DgmLen:40
******S* Seq: 0x2A9F61BD  Ack: 0x0  Win: 0x800  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-18:05:45.407380 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:3 TCP TTL:57 TOS:0x0 ID:57895 IpLen:20 DgmLen:40
******S* Seq: 0x2A9F61BD  Ack: 0x0  Win: 0x800  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-18:05:45.421634 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:4 TCP TTL:57 TOS:0x0 ID:14182 IpLen:20 DgmLen:40
******S* Seq: 0x2A9F61BD  Ack: 0x0  Win: 0x800  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Nmap SYN/FIN Scan

B. Nmap NULL Scan

C. Nmap ACK Scan

D. Nmap SYN Scan

E. Nmap XMAS Scan

ANSWER: D

QUESTION NO: 8

What is the name of the informational page that is relevant to a particular command in

Linux?

A. Readme Page

B. Lnx_nfo Page

C. Man Page

D. X_Win Page

E. Cmd_Doc Page

ANSWER: C

Often times attackers will run scans against the network to identify different network and operating systems, and resources that are available. If an attacker runs scans on the network, and you are logging the connections, which of the following represent the legitimate combination of packets that will be sent between the attacker and target?

A. Attacker PSH-FIN Scan, Target RST-FIN Response

B. Attacker ACK Scan, Target NULL Response

C. Attacker NULL Scan, Target RST Response

D. Attacker SYN Scan, Target NULL Response

E. Attacker FIN Scan, Target RST Response

ANSWER: C E

Which of the following equation pairs show examples of an Inverse Function?

A. 20+3=23 and 23-3=20

B. 10*2=20 and 20/2=10

C. 20*2=40 and 40*0.5=20

D. 40/2=20 and 20/0.5=40

E. 30+10=40 and 40-10=30

F. 10*2=20 and 20*0.5=10

ANSWER: A B E

You are working on the authentication systems in your network, and are concerned with your legacy systems. In Windows NT 4.0, before Service Pack 4 (SP4), there were only two supported methods of authentication. What were those two methods?

A. NetBIOS

B. LM

C. NTLM

D. NTLMv2

E. Kerberos

ANSWER: B C

QUESTION NO: 12

You have just finished installing new servers and clients in your office network. All the new client machines are running Windows 2000 Professional, and the servers are running Windows Server 2003. You are now working on securing all user authentication related areas of the systems. Where is user account information stored, both for the Domain and the local machine?
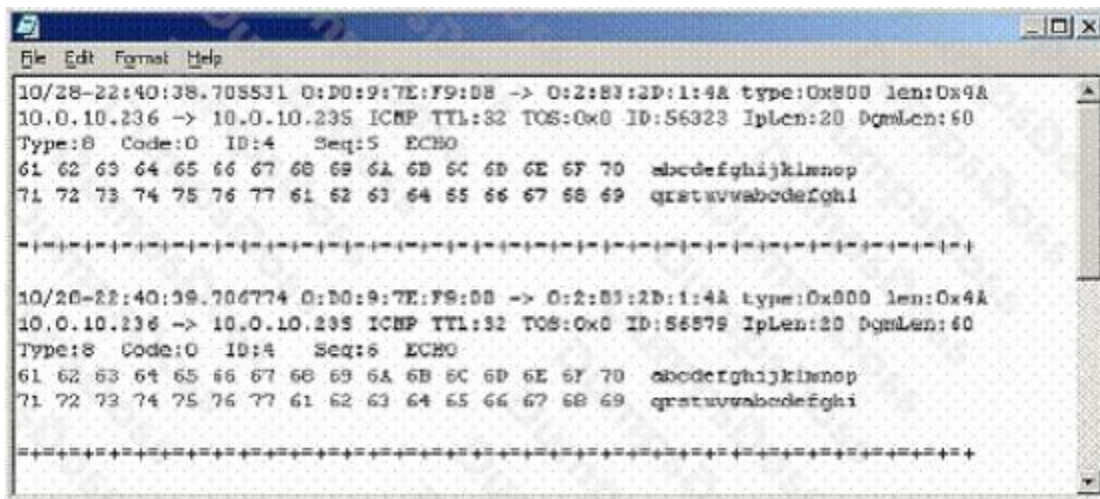
A. Domain user account information is stored in the Active Directory.

B. Local user account information is stored in the SAM.

C. Local user account information is stored in the Active Directory.

D. Domain user account information is stored in the SAM.

E. Domain user account information is stored in the Metabase

ANSWER: A B

QUESTION NO: 13

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```
10/28-22:40:38.705531 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56323 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:5  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70   abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/28-22:40:39.706774 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56579 IpLen:20 DgmLen:60
Type:8  Code:0  ID:4   Seq:6  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70   abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Windows 2000 Ping Request

B. Windows NT 4.0 Ping Request

C. Linux Ping Request

D. Linux Ping Response

E. Windows NT 4.0 Ping Response

ANSWER: B

QUESTION NO: 14

From the following list, chose the primary reason for splitting a Security Policy into multiple smaller policies?

A. Smaller policies are cheaper to produce

B. Smaller policies are simpler to manage

C. Smaller policies are simpler to produce

D. Smaller policies are more legally binding

E. Smaller policies provide better security control

ANSWER: B

QUESTION NO: 15

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```
File  Edit  Format  Help
10/27-23:48:42.126886 0:D0:9:7E:E5:E9 -> 0:D0:9:7F:C:9B type:0x800 len:0x3C
10.0.10.237 -> 10.0.10.234 ICMP TTL:128 TOS:0x0 ID:1185 IpLen:20 DgmLen:36
Type:8  Code:0  ID:3    Seq:289   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:48:42.137906 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.237 -> 10.0.10.235 ICMP TTL:128 TOS:0x0 ID:1186 IpLen:20 DgmLen:36
Type:8  Code:0  ID:3    Seq:290   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:48:42.148642 0:D0:9:7E:E5:E9 -> 0:D0:9:7E:F9:DB type:0x800 len:0x3C
10.0.10.237 -> 10.0.10.236 ICMP TTL:128 TOS:0x0 ID:1187 IpLen:20 DgmLen:36
Type:8  Code:0  ID:3    Seq:291   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:48:42.167031 0:D0:9:7E:E5:E9 -> 0:D0:9:68:87:2C type:0x800 len:0x3C
10.0.10.237 -> 10.0.10.238 ICMP TTL:128 TOS:0x0 ID:1190 IpLen:20 DgmLen:36
Type:8  Code:0  ID:3    Seq:292   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

10/27-23:48:42.177247 0:D0:9:7E:E5:E9 -> 0:D0:9:69:48:E3 type:0x800 len:0x3C
10.0.10.237 -> 10.0.10.239 ICMP TTL:128 TOS:0x0 ID:1191 IpLen:20 DgmLen:36
Type:8  Code:0  ID:3    Seq:293   ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A. Nmap Scan

B. Port Scan

C. Trojan Scan

D. Ping Request

E. Ping Sweep

ANSWER: E