

Vendor: EXIN

Exam Code: SCNP

Exam Name: SCNP Strategic Infrastructure Security

Version: Demo

QUESTION NO: 1

In the process of public key cryptography, which of the following is true?

- A. Only the public key is used to encrypt and decrypt
- B. Only the private key can encrypt and only the public key can decrypt
- C. Only the public key can encrypt and only the private key can decrypt
- D. The private key is used to encrypt and decrypt
- E. If the public key encrypts, then only the private key can decrypt

Answer: E

QUESTION NO: 2

As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Physical and Environmental Security?

- A. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.
- B. The objectives of this section are to prevent unauthorized access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities.
- C. The objectives of this section are to provide management direction and support for information security.
- D. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
- E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Answer: B

QUESTION NO: 3

During a one week investigation into the security of your network you work on identifying the information that is leaked to the Internet, either directly or indirectly. One thing you decide to evaluate is the information stored in the Whois lookup of your organizational website. Of the following, what pieces of information can be identified via this method?

- A. Registrar

-
- B. Mailing Address
 - C. Contact Name
 - D. Record Update
 - E. Network Addresses (Private)

Answer: A,B,C,D

QUESTION NO: 4

You are aware of the significance and security risk that Social Engineering plays on your company. Of the following Scenarios, select those that, just as described, represent potentially dangerous Social Engineering:

- A. A writer from a local college newspapers calls and speaks to a network administrator. On the call the writer requests an interview about the current trends in technology and offers to invite the administrator to speak at a seminar.
- B. An anonymous caller calls and wishes to speak with the receptionist. On the call the caller asks the receptionist the normal business hours that the organization is open to the public.
- C. An anonymous caller calls and wishes to speak with the purchaser of IT hardware and software. On the call the caller lists several new products that the purchaser may be interested in evaluating. The caller asks for a time to come and visit to demonstrate the new products.
- D. An email, sent by the Vice President of Sales and Marketing, is received by the Help Desk asking to reset the password of the VP of Sales and Marketing.
- E. An email is received by the Chief Security Officer (CSO) about a possible upgrade coming from the ISP to a different brand of router. The CSO is asked for the current network's configuration data and the emailer discusses the method, plan, and expected dates for the rollover to the new equipment.

Answer: D,E

QUESTION NO: 5

During the review of the security logs you notice some unusual traffic. It seems that a user has connected to your Web site ten times in the last week, and each time has visited every single page on the site. You are concerned this may be leading up to some sort of attack. What is this user most likely getting ready to do?

- A. Mirror the entire web site.
- B. Download entire DNS entries.
- C. Scan all ports on a web server.

-
- D. Perform a Distributed Denial of Service attack through the Web server.
 - E. Allow users to log on to the Internet without an ISP.

Answer: A

QUESTION NO: 6

What type of cipher is used by an algorithm that encrypts data one bit at a time?

- A. 64-bit encryption Cipher
- B. Block Cipher
- C. Stream Cipher
- D. Diffuse Cipher
- E. Split Cipher

Answer: C

QUESTION NO: 7

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 Secedit.exe?

- A. This tool is used to set 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 NTFS security.
- 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: C

QUESTION NO: 8

To increase the security of your network and systems, it has been decided that EFS will be implemented in the appropriate situations. Two users are working on a common file, and often email this file back and forth between each other. Is this a situation where the use of EFS will create effective security, and why (or why not)?

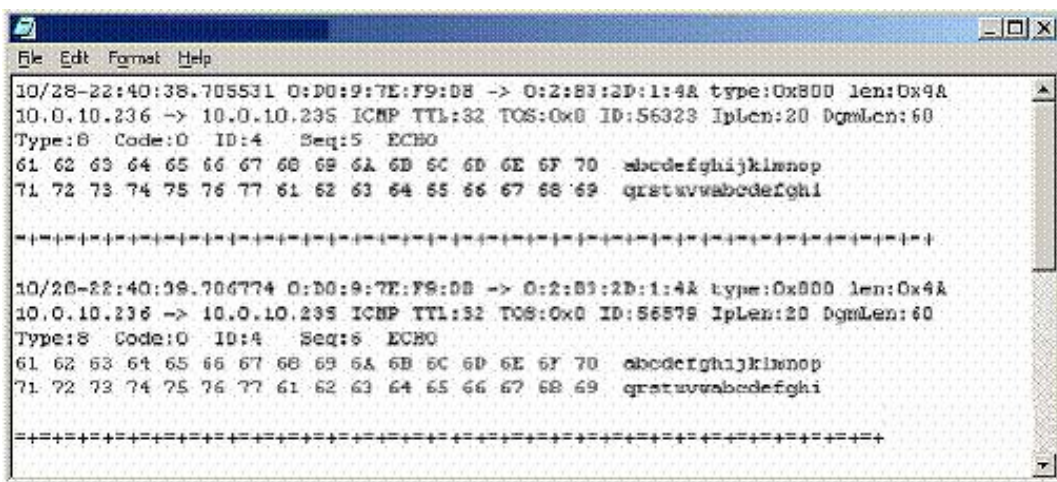
- A. No, the security will remain the same since both users will share the same key for encryption.

-
- B. Yes, since the file will be using two keys for encryption the security will increase.
 - C. No, the security will remain the same since both users will share the same key for decryption.
 - D. Yes, since the file will be using two keys for decryption the security will increase.
 - E. No, EFS cannot be used for files that are shared between users.

Answer: E

QUESTION NO: 9

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
10/28-22:40:38.705531 0:00:9:7E:F9:08 -> 0:2:83:2D: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

-----

10/28-22:40:38.706774 0:00:9:7E:F9:08 -> 0:2:83:2D:1:4A type:0x800 len:0x4A
10.0.10.238 -> 10.0.10.235 ICMP TTL:32 TOS:0x0 ID:56579 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

-----
```

- 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: 10

In order for your newly written security policy to have any weight, it must be implemented. Which of the following are the three components of a successful Security Policy Implementation in an organization?

- A. Policy Monitoring
- B. Policy Design
- C. Policy Committee
- D. Policy Enforcement

E. Policy Documentation

Answer: A,B,D

QUESTION NO: 11

Attackers have the ability to use programs that are able to reveal local passwords by placing some kind of a pointer/cursor over the asterisks in a program's password field. The reason that such tools can uncover passwords in some Operating Systems is because:

- A. the passwords are simply masked with asterisks
- B. the etc/passwd file is on a FAT32 partition
- C. the passwords are decrypted on screen
- D. the password text is stored in ASCII format
- E. the etc/passwd file is on a FAT16 partition

Answer: A

QUESTION NO: 12

To maintain the security of your network you routinely run several checks of the network and computers.

Often you use the built-in tools, such as netstat. If you run the following command: netstat -e which of the following will be the result?

- A. Displays all connections and listening ports
- B. Displays Ethernet statistics
- C. Displays addresses and port numbers in numerical form
- D. Shows connections for the protocol specified
- E. Displays per-protocol statistics

Answer: B

QUESTION NO: 13

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: 14

What is a problem with symmetric key cryptography?

- A. It is slower than asymmetric key cryptography
- B. Secure distribution of the public key
- C. There is a lack of encryption protocols that can use symmetric key cryptography
- D. Secure distribution of a secret key
- E. Symmetric key cryptography is reserved for the NSA

Answer: D

QUESTION NO: 15

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

QUESTION NO: 16

You have just downloaded a new file, called scnpfile.tar.gz. You are going to verify the file prior to un-archiving the file. Which command do you need to type to un-compress the file, prior to un-archiving?

-
- A. tar xvf scnpfile.tar.gz
 - B. tar -zxvf scnpfile.tar.gz
 - C. gunzip scnpfile.tar.gz
 - D. gunzip -xvf scnpfile.tar.gz
 - E. gunzip -zxvf scnpfile.tar.gz

Answer: C

QUESTION NO: 17

You are configuring the lines that control access to exported objects on your server running NFS. If you have a directory called /Tech and you wish to export this directory to network 192.168.20.0/24, allowing root access, and the permissions of read and write, which of the following lines will accomplish this?

- A. (RW) no_root_squash /Tech 192.168.20.0/24
- B. /Tech 192.168.20.0/24 (rw) no_root_squash
- C. (RW) no_root_squash 192.168.20.0/24 /Tech
- D. (RW)no_root_squash:/Tech 192.168.20.0/24
- E. /Tech 192.168.20.0/24(rw) no_root_squash

Answer: E

QUESTION NO: 18

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: 19

If you encrypt or decrypt files and folders located on a remote computer that has been enabled for remote encryption; the data that is transmitted over the network by this process is not encrypted. In order to keep data encrypted as it is transmitted over the network, which of the following must

-
- D. Port Scan
 - E. Ping Sweep

Answer: D

QUESTION NO: 21

As per the guidelines in the ISO Security Policy standard, what is the purpose of the section on Business Continuity Planning?

- A. The objectives of this section are to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.
- B. The objectives of this section are to provide management direction and support for information security.
- C. The objectives of this section are to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.
- D. The objectives of this section are to avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements, and to ensure compliance of systems with organizational security policies and standards.
- E. The objectives of this section are to control access to information, to prevent unauthorized access to information systems, to ensure the protection of networked services, and to prevent unauthorized computer access.

Answer: C

QUESTION NO: 22

On Monday, during a routine check of a users Windows workstation, you find the following program, called regedit.bat on the users local hard drive:

```
Net localgroup administrators local /all
```

```
Start regedit.exe
```

```
Exit
```

What is this program capable of doing on this computer?

- A. Nothing, the first line is coded wrong.
- B. It will add the administrators to the local group
- C. It will add the local user to all local groups
- D. It will add the administrators to all local groups
- E. It will add the local user to the administrators group

Answer: E

QUESTION NO: 23

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

QUESTION NO: 24

You are discussing the design and infrastructure of the Internet with several colleagues when a disagreement begins over the actual function of the NAP in the Internets design. What is the function of a NAP in the physical structure of the Internet?

- A. The NAP provides for a layered connection system of ISPs connecting to the backbone.
- B. The NAP provides the actual connection point between a local user and the Internet.
- C. The NAP provides the physical network with communication channels for the Internet and voice/data applications.
- D. The NAP provides a national interconnection of systems, called peering centers, to the NSPs.
- E. The NAP provides for a connection point between an ISP and the backbone of the Internet.

Answer: E

QUESTION NO: 25

When using the 3DES encryption ($C = EK_1[DK_2[EK_1[P]]]$) , what is the function of C?

- A. C is the text before encryption
- B. C is the first encryption key
- C. C is the second encryption key
- D. C is the decryption key
- E. C is the text after encryption

Answer: E

QUESTION NO: 26

Which of the following are symmetric encryption algorithms?

- A. MD5
- B. RSA
- C. Diffie-Hellman
- D. 3DES
- E. AES

Answer: D,E

QUESTION NO: 27

During the configuration of your Linux system, you are working with the available drives in the computer.

What syntax defines the First (Primary) IDE hard disk drive?

- A. /dev/sda
- B. /dev/fda
- C. /dev/hd1
- D. /dev/hda
- E. /dev/fd1

Answer: D

QUESTION NO: 28

You are configuring the permissions to a file, called file1, on your Linux file server. You wish to change the permissions to remove the execute permission from the others and group. Which of the following commands will complete this task?

- A. umask x-og file1
- B. umask og-x file1
- C. chmod xog- file1
- D. chmod x-og file1
- E. chmod og-x file1

Answer: E

QUESTION NO: 29

In the past it was, at times, difficult to locate current information on security vulnerabilities. What is the name of the security community's effort to create a comprehensive database of multiple vulnerabilities and security tools?

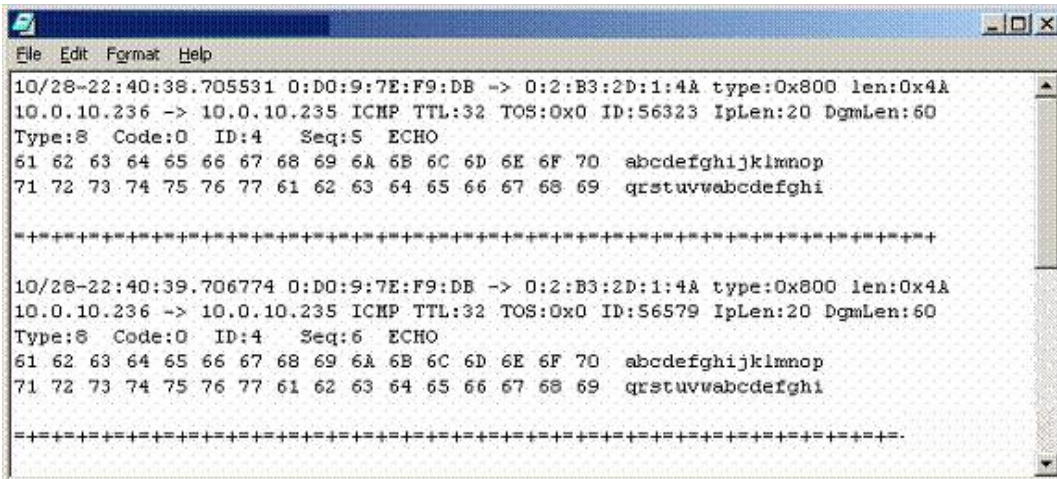
- A. Common Vulnerabilities and Exploits
- B. Cataloged Vulnerabilities and Exposures
- C. Common Vulnerabilities and Exposures
- D. Cataloged Vulnerabilities and Exposures
- E. Cataloged Vulnerabilities and Exploits

Answer: C

QUESTION NO: 30

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:DD:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICHP 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:DD:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x4A
10.0.10.236 -> 10.0.10.235 ICHP 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

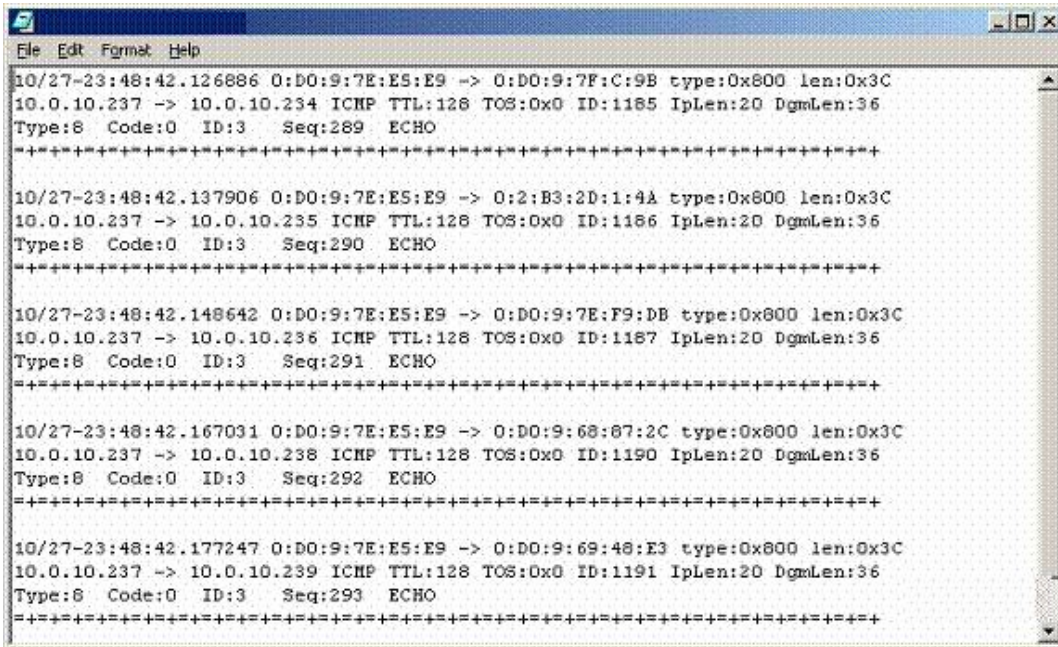
=====
```

- 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: 31

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

QUESTION NO: 32

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
10/27-23:56:37.033614 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3469 -> 10.0.10.235:1 TCP TTL:128 TOS:0x0 ID:1315 IpLen:20 DgmLen:48
*****S* Seq: 0x17CA2EE3 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.042943 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3470 -> 10.0.10.235:2 TCP TTL:128 TOS:0x0 ID:1316 IpLen:20 DgmLen:48
*****S* Seq: 0x17CAD3B4 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.052969 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3471 -> 10.0.10.235:3 TCP TTL:128 TOS:0x0 ID:1317 IpLen:20 DgmLen:48
*****S* Seq: 0x17CB969A Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.062946 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3472 -> 10.0.10.235:4 TCP TTL:128 TOS:0x0 ID:1318 IpLen:20 DgmLen:48
*****S* Seq: 0x17CC52C7 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.072986 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3473 -> 10.0.10.235:5 TCP TTL:128 TOS:0x0 ID:1319 IpLen:20 DgmLen:48
*****S* Seq: 0x17CD1091 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.082983 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3474 -> 10.0.10.235:6 TCP TTL:128 TOS:0x0 ID:1320 IpLen:20 DgmLen:48
*****S* Seq: 0x17CDEF72 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/27-23:56:37.093010 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:3475 -> 10.0.10.235:7 TCP TTL:128 TOS:0x0 ID:1321 IpLen:20 DgmLen:48
*****S* Seq: 0x17CEB24E Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
```

- A. NetBus Scan
- B. Trojan Scan
- C. Ping Sweep
- D. Port Scan
- E. Ping Sweep

Answer: D

QUESTION NO: 33

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
10/28-01:07:09.684971 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1709 -> 10.0.10.235:12345 TCP TTL:128 TOS:0x0 ID:5443 IpLen:20 DgmLen:48
*****S* Seq: 0x4C8E418E Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.695924 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1710 -> 10.0.10.235:20034 TCP TTL:128 TOS:0x0 ID:5444 IpLen:20 DgmLen:48
*****S* Seq: 0x4C8EFBAD Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.705251 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1711 -> 10.0.10.235:23456 TCP TTL:128 TOS:0x0 ID:5445 IpLen:20 DgmLen:48
*****S* Seq: 0x4C902D65 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.715301 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1712 -> 10.0.10.235:27374 TCP TTL:128 TOS:0x0 ID:5446 IpLen:20 DgmLen:48
*****S* Seq: 0x4C90C6A3 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.725111 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1713 -> 10.0.10.235:30029 TCP TTL:128 TOS:0x0 ID:5447 IpLen:20 DgmLen:48
*****S* Seq: 0x4C91BA3D Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.734845 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1714 -> 10.0.10.235:30999 TCP TTL:128 TOS:0x0 ID:5448 IpLen:20 DgmLen:48
*****S* Seq: 0x4C927D89 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:07:09.739681 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1715 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5449 IpLen:20 DgmLen:48
*****S* Seq: 0x4C92E2CC Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
```

- A. Port Scan
- B. Trojan Scan
- C. Back Orifice Scan
- D. NetBus Scan
- E. Ping Sweep

Answer: B

QUESTION NO: 34

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?


```
[**] ICMP test [**]
OS/26-03:18:29.700732 10.0.10.113 -> 10.0.10.213
ICMP TTL:128 TOS:0x0 ID:9466 IpLen:20 DgmLen:60
Type:8 Code:0 ID:2 Seq:34 ECHO
0x0000: 00 02 B3 2D 01 4A 00 02 B3 25 50 09 08 00 45 00  ...-.J...%P...E.
0x0010: 00 3C 24 FA 00 00 80 01 EC 81 0A 00 0A 71 0A 00  .<$.....q..
0x0020: 0A D5 08 00 29 5C 02 00 22 00 61 62 63 64 65 66  ....)\...".abcdef
0x0030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040: 77 61 62 63 64 65 66 67 68 69                    wabcdefghi

-----

[**] ICMP test [**]
OS/26-03:18:30.699457 10.0.10.113 -> 10.0.10.213
ICMP TTL:128 TOS:0x0 ID:9467 IpLen:20 DgmLen:60
Type:8 Code:0 ID:2 Seq:35 ECHO
0x0000: 00 02 B3 2D 01 4A 00 02 B3 25 50 09 08 00 45 00  ...-.J...%P...E.
0x0010: 00 3C 24 FB 00 00 80 01 EC 80 0A 00 0A 71 0A 00  .<$.....q..
0x0020: 0A D5 08 00 28 5C 02 00 23 00 61 62 63 64 65 66  ....(\...#.abcdef
0x0030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040: 77 61 62 63 64 65 66 67 68 69                    wabcdefghi

-----
```

- A. Linux Ping Reply
- B. Windows 2000 Ping Reply
- C. Windows NT 4.0 Ping Request
- D. Linux Ping Request
- E. Windows 2000 Ping Request

Answer: E

QUESTION NO: 35

It has come to your attention that some machine has tried to send a packet to your DNS server containing both a DNS query and an answer that is false. What type of attack was used against your network?

- A. DNS overflow
- B. DNS poisoning through sequence prediction
- C. Statd overflow
- D. DNS cache poisoning
- E. DNS parse corruption

Answer: D

QUESTION NO: 36

What type of an attack would someone be using if they sent a packet to their target with identical source and destination IP address and port (which is the address of the target machine) which can

cause a system to go into an infinite loop trying to complete a connection?

- A. SYN loop
- B. WinNuke
- C. SYN flood
- D. Ping of death
- E. Land attack

Answer: E

QUESTION NO: 37

You are examining a packet from an unknown host that was trying to ping one of your protected servers and notice that the packets it sent had an IPLen of 20 bytes and DgmLen set to 60 bytes. What type of operating system should you believe this packet came from?

- A. Linux
- B. SCO
- C. Windows
- D. Mac OSX
- E. Netware

Answer: C

QUESTION NO: 38

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
10/28-01:52:16.979681 0:D0:9:7E:E5:E9 -> 0:D0:9:7F:C:9B type:0x800 len:0x3E
10.0.10.237:1674 -> 10.0.10.234:31337 TCP TTL:128 TOS:0x0 ID:5277 IpLen:20 DgmLen:48
*****S* Seq: 0x3F2FE2CC Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:52:16.999652 0:D0:9:7E:E5:E9 -> 0:2:B3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1675 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5278 IpLen:20 DgmLen:48
*****S* Seq: 0x3F30D51F Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:52:17.019680 0:D0:9:7E:E5:E9 -> 0:D0:9:7E:F9:DB type:0x800 len:0x3E
10.0.10.237:1676 -> 10.0.10.236:31337 TCP TTL:128 TOS:0x0 ID:5279 IpLen:20 DgmLen:48
*****S* Seq: 0x3F3183AE Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:52:17.059669 0:D0:9:7E:E5:E9 -> 0:D0:9:68:87:2C type:0x800 len:0x3E
10.0.10.237:1678 -> 10.0.10.238:31337 TCP TTL:128 TOS:0x0 ID:5282 IpLen:20 DgmLen:48
*****S* Seq: 0x3F332EC2 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+
10/28-01:52:17.079821 0:D0:9:7E:E5:E9 -> 0:D0:9:69:48:E3 type:0x800 len:0x3E
10.0.10.237:1679 -> 10.0.10.239:31337 TCP TTL:128 TOS:0x0 ID:5283 IpLen:20 DgmLen:48
*****S* Seq: 0x3F3436FA Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
+-----+

```

- A. Trojan Horse Scan
- B. Back Orifice Scan
- C. NetBus Scan
- D. Port Scan
- E. Ping Sweep

Answer: B

QUESTION NO: 39

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
10/28-17:28:06.234410 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x62
10.0.10.233 -> 10.0.10.235 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:2116 Seq:0 ECHO
F1 98 DC 3B E7 13 02 00 08 09 0A 0B 0C 0D 0E 0F ...;.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#%&'()*+,-./
30 31 32 33 34 35 36 37 01234567
+-----+
10/28-17:28:07.231774 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x62
10.0.10.233 -> 10.0.10.235 ICMP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:2116 Seq:1 ECHO
F2 98 DC 3B 6D 0A 02 00 08 09 0A 0B 0C 0D 0E 0F ...;#.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#%&'()*+,-./
30 31 32 33 34 35 36 37 01234567
+-----+

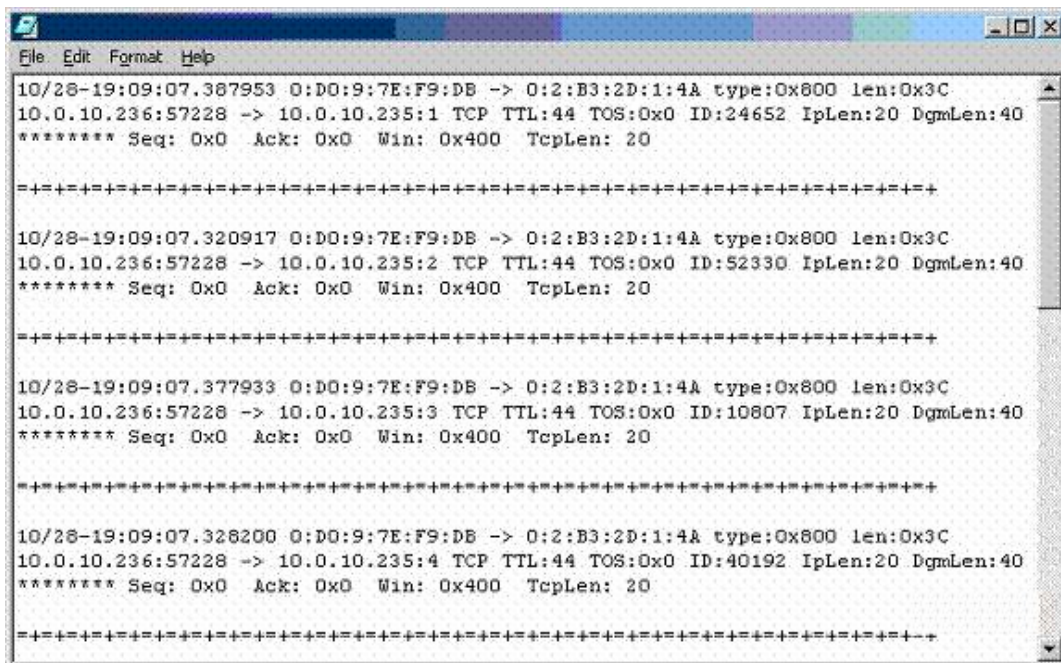
```

- A. Linux Ping Response
- B. Linux Ping Request
- C. Windows 2000 Ping Request
- D. Windows 2000 Ping Response
- E. Windows NT 4.0 Ping Request

Answer: B

QUESTION NO: 40

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
10/28-19:09:07.387953 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:57228 -> 10.0.10.235:1 TCP TTL:44 TOS:0x0 ID:24652 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.320917 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:57228 -> 10.0.10.235:2 TCP TTL:44 TOS:0x0 ID:52330 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.377933 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:57228 -> 10.0.10.235:3 TCP TTL:44 TOS:0x0 ID:10807 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.328200 0:D0:9:7E:F9:DB -> 0:2:B3:2D:1:4A type:0x800 len:0x3C
10.0.10.236:57228 -> 10.0.10.235:4 TCP TTL:44 TOS:0x0 ID:40192 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
```

- A. Nmap SYN/FIN Scan
- B. Nmap ACK Scan
- C. Nmap NULL Scan
- D. Nmap XMAS Scan
- E. Nmap SYN Scan

Answer: C

QUESTION NO: 41

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?

-
- A. Nmap XMAS Scan
 - B. Nmap NULL Scan
 - C. Nmap SYN Scan
 - D. Nmap ACK Scan
 - E. Nmap SYN/FIN Scan

Answer: A

QUESTION NO: 43

Recently you have had meetings with an organization to design their security policy. There has been some resistance on their board concerning the need for a security policy. To help remove the resistance, you describe the many benefits to having a security policy. Which of the following are the benefits of a security policy?

- A. Help to prevent misuse of resources
- B. Help to decrease the legal liability
- C. Help to protect proprietary information
- D. Help to lower bandwidth usage
- E. Help protect data from unauthorized access

Answer: A,B,C,E

QUESTION NO: 44

You are forming the security policy for your organization. You have identified those in the organization who will participate in the creation of the policy. Several of the people you have contacted wish to know what will be on the agenda during the first meeting. During the very first policy design meeting, which of the following issues will you tell those in the policy committee to discuss?

- A. Identification of the critical business resources
- B. Identification of the infrastructure architecture
- C. Determination of the type of policy to create
- D. Identification of the critical business policies
- E. Determination of the critical policies of key connected business partners

Answer: A,C,D

QUESTION NO: 45

You are creating the User Account section of your organizational security policy. From the following options, select the questions to use for the formation of this section?

- A. Are users allowed to make copies of any operating system files (including, but not limited to /etc/passwd or the SAM)?
- B. Who in the organization has the right to approve the request for new user accounts?
- C. Are users allowed to have multiple accounts on a computer?
- D. Are users allowed to share their user account with coworkers?
- E. Are users required to use password-protected screensavers?
- F. Are users allowed to modify files they do not own, but have write abilities?

Answer: B,C,D

QUESTION NO: 46

You have been given the task of writing your organizations security policy. During your research you find that there are several established standards for security policy design. Which of the following are accepted standards?

- A. ISO 17799
- B. BS 197
- C. ISO 979
- D. BS 7799
- E. ISO 179

Answer: A,D

QUESTION NO: 47

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: 48

You are creating the Remote Access section of your organizational security policy. From the following options, select the questions to use for the formation of this section?

- A. What methods of remote access are allowed (cable modem, DSL, and so on)?
- B. How are partner VPNs to be configured (to firewall or host)?
- C. Which users are authorized to install networking devices into computers?
- D. What is the process for becoming authorized for remote access?
- E. Is the entire network accessible remotely?

Answer: A,D,E

QUESTION NO: 49

Recently at your organization you have been requested to lead the team in performing a new Risk Analysis of the organization. During the first team meeting you identify to your team the three areas of Risk Analysis. What are those three areas?

- A. Verifying Risk, Minimizing Risk, Removing Risk
- B. Qualifying Risk, Mitigating Risk, Removing Risk
- C. Predicating Risk, Qualifying Risk, Minimizing Risk
- D. Predicting Risk, Quantifying Risk, Mitigating Risk
- E. Quantifying Risk, Mitigating Risk, Removing Risk

Answer: D

QUESTION NO: 50

Your organization assigns an Annual Loss Expectancy to assets during a risk analysis meeting. You have a server which if down for a day will lose the company \$25,000, and has a serious root access attack against it once per month. What is the ALE for this attack against this server?

- A. \$25,000
- B. \$300,000
- C. \$120,000
- D. \$2,083
- E. \$2,500

Answer: B

QUESTION NO: 51

Which two of the following are factors that must be considered in determining the likelihood of occurrence during a risk analysis review?

- A. What are the methods available to attack this asset?
- B. What are the costs associated with protecting this asset?
- C. Does the threat have sufficient capability to exercise the attack?
- D. Does the threat have the motivation or incentive to exercise the attack?
- E. Are any of the assets worthy of an attack?

Answer: C,D

QUESTION NO: 52

After a security meeting, IT leaders decided that the organization will perform a completely new risk analysis, as the previous one was done over five years ago. The methods that will be used is FRAP. Which of the following best describes the FRAP method of risk analysis?

- A. FRAP involves assigning team members to identify specific vulnerabilities. Once the vulnerabilities have been identified, a level of risk is assigned, as a factor of times per year this vulnerability may be exploited. Finally, a dollar value in lost revenue is assigned to each asset that can be compromised by this vulnerability.
- B. FRAP is a team method. Individuals from different aspects of an organization form a committee. Once together, they discuss the areas of risk, the likelihood of a threat, the impact of the threat, and the methods that should be used to minimize the threat.
- C. FRAP involves assigning dollar values to assets, and calculating how often a threat to the asset will occur. Once determined an approximate dollar value to each asset and threat combination is calculated.
- D. FRAP is the process of determining the likelihood of a threat as medium, high, or low. Once the likelihood is determined the cost is identified, again as medium, high, or low. Finally, based on cost, a response to the threat is determined.
- E. FRAP is the process of determining the likelihood of a threat as medium, high, or low. Once the likelihood is determined, the level of damage is identified, again as high, medium, or low. Finally, the response to the threat is determined.

Answer: B

QUESTION NO: 53

Your organization assigns an Annual Loss Expectancy to assets during a risk analysis meeting. You have a server which if down for a day will lose the company \$35,000, and has a serious root access attack against it once per month. What is the ALE for this attack against this server?

- A. \$35,000
- B. \$120,000
- C. \$2,916
- D. \$3,500
- E. \$420,000

Answer: E

QUESTION NO: 54

Which of the following best describes the Repair Model?

A. The model makes use of preventive measures and regular service as well as updates such as Service

Packs, maintenance updates, and patches. Preventive measures can also improve the chances of the repair model working better than if the system had no preventive measures ever taken.

B. The repair model is the transference of risk to an insurance company that covers the costs of replacing the critical assets within your network. The drawbacks are increase in premiums after making a claim, high premiums anyway, down time while the insurance company is processing the claim, and claim may not pay what replacement costs are today.

C. Assets will typically cost much more than the original capital outlay that it took to purchase it long ago.

Repair costs can be very high and a decision to exercise this model should not be made in haste. There are also depreciation issues to deal with as well. In any case, this model should be the last resort because of cost and may be the most time consuming.

D. The repair model makes use of the acknowledged skills and abilities of the existing personnel. Knowing that assets have very specific dollar values assigned to them, the choice on how to manage the asset is based on the experience of the personnel.

E. Before incurring the cost for repair of an inoperative asset, check for maintenance agreements that may include the cost of repair or the actual repair itself. Nevertheless, the repair model should focus on the restoration of the downed asset to its working status within the network infrastructure. Keep in mind that after hardware costs, costs for the reloading or replacement of software can be a large cost factor as well.

Answer: E

QUESTION NO: 55

Which of the following has the stages of Risk Analysis in order, from a to e?

- a) Management
- b) Threat Assessment
- c) Control Evaluation
- d) Inventory
- e) Monitoring

- A. b, d, c, e, a
- B. a, b, d, c, e
- C. d, b, c, a, e
- D. a, b, c, d, e
- E. d, b, a, c, e

Answer: C

QUESTION NO: 56

You have just recently finished a complete Risk Analysis of your organization. During your presentation you present the controls you feel must be implemented. Which is considered to be the major factor in determining a specific control system to implement?

- A. Control system documentation
- B. Return on investment
- C. Current system availability
- D. Familiarity with the system
- E. Staffs previous use of system

Answer: B

QUESTION NO: 57

During a discussion of asset classification and protection with a coworker, you realize that your coworker does not know the basic concepts of asset protection. You are asked to describe the types of asset protection. Which of the following describes the concept of feasible protection of an asset?

- A. The cost to replace the asset is greater than the cost of recovery of the asset.
- B. The cost to replace the asset is less than the cost of protect the asset.
- C. The cost to protect the asset is greater than the cost of recovery of the asset.
- D. The cost to replace the asset is less than the cost of recovery of the asset.
- E. The cost to protect the asset is less than the cost of recovery of the asset.

Answer: E

QUESTION NO: 58

To manage the risk analysis of your organization you must first identify the method of analysis to use.

Which of the following organizations defines the current standards of risk analysis methodologies?

- A. NIST
- B. CERT
- C. F-ICRC
- D. NBS
- E. NSA

Answer: A

QUESTION NO: 59

You are running a Linux machine as a dedicated file server for your network. You are trying to use Nmap to perform some security tests. On your Linux machine, in order to run TCP SYN scans from a host using Nmap or NmapFE you must have which of the following?

- A. telnet access
- B. root privileges
- C. access to tcpdump
- D. login access to a router
- E. login access to the target

Answer: B

QUESTION NO: 60

One of your users calls to state the their computer is acting unusual. You go to investigate and find there is an unauthorized program installed on this computer. You examine the network and find that this program has replicated itself to other machines in the network, without the input of the user. What type of program is in the network?

- A. The program is a Worm.
- B. The program is a Virus.
- C. The program is a Bug.
- D. The program is a Trojan Horse.

E. The program is a Macro.

Answer: A

QUESTION NO: 61

If an attacker uses a program that sends thousands of email messages to every user of the network, some of them with over 50MB attachments. What are the possible consequences to the email server in the network?

- A. Server hard disk can fill to capacity
- B. Client hard disks can fill to capacity
- C. Server can completely crash
- D. Network bandwidth can be used up
- E. Clients cannot receive new email messages

Answer: A,C

QUESTION NO: 62

Your network has been hit by a virus that is infecting the MBR on many of the systems in the network.

You are working to repair the damage this virus has done. After two days of non-stop work on the problem, you get things under control. What type of virus was in your network?

- A. Macro Virus
- B. Scripting Virus
- C. Boot Sector Virus
- D. Multi-part Virus
- E. File Infection Virus

Answer: C

QUESTION NO: 63

Your network has been hit by a very bad virus recently. As you tracked the virus through the network, it was changing from system, to system. Each time it went to infect a system; it had evolved slightly to have a different file size, or different file structure. After extensive work, you and your team were able to isolate and remove the virus from the network. Which of the following best identifies the type of virus that was in your network?

-
- A. Boot Sector Virus
 - B. Macro Virus
 - C. Stealth Virus
 - D. Multi-part Virus
 - E. Polymorphic Virus

Answer: E

QUESTION NO: 64

You are running some tests in your network, to see if you can remotely identify the operating system of nodes in the network. Using the nmap tool, which of the following commands will identify the operating system of the computer using IP address 192.168.10.1?

- A. nmap -ident 192.168.10.1 -sS
- B. nmap -sS 192.168.10.1 -O
- C. nmap -ld 192.168.10.1 -sS
- D. nmap -a -u -x -ld 192.168.10.1
- E. nmap -ld 192.168.10.1 -aux -sS

Answer: B

QUESTION NO: 65

You are running Nessus in your organization to perform vulnerability assessments. If you wish to write your own plugin, to scan for a custom vulnerability, what will you use to write the plugin?

- A. Nessus Plugin Scripting (NPS)
- B. Nessus Custom Scripting (NCS)
- C. Nessus C++ Scripting (NC+S)
- D. Nessus Attack Scripting Language (NASL)
- E. Nessus Java Scripting Language (NJSL)

Answer: D

QUESTION NO: 66

You have recently started using Nessus to perform vulnerability scans on the systems in your network.

You now wish to perform further testing, to ensure that passwords are the proper length in the network.

What feature of Nessus allows you to perform this type of custom scanning?

-
- A. Nessus Plugins
 - B. Nessus cannot perform this type of scan, it is restricted to vulnerability scanning
 - C. Nessus Advanced Scripting
 - D. Nessus Password Scanning Module
 - E. Nessus Policies

Answer: E

QUESTION NO: 67

To maintain the security of your network you routinely run several checks of the network and computers.

Often you use the built-in tools, such as netstat. If you run the following command, netstat -s which of the following will be the result?

- A. Displays all connections and listening ports
- B. Displays Ethernet statistics.
- C. Displays addresses and port numbers in numerical form
- D. Shows connections for the protocol specified
- E. Displays per-protocol statistics

Answer: E

QUESTION NO: 68

You have just finished running vulnerability test, using Nessus, on a remote host in your network. You are reading the report Nessus generated, and are looking for those items you must address right away. In a

Nessus report, how are items marked that require your immediate attention?

- A. With a Yellow Exclamation Point
- B. With a Red X
- C. With a Black check
- D. With a Yellow check
- E. With a bulls-eye target

Answer: B

QUESTION NO: 69

In order to run some tests on your system, you have decided to use the netcat utility. You want to be able to access the command prompt on a Windows system from your Linux system. What is

the proper command on the Windows system to allow for you to gain remote access?

- A. netcat -p 2020 -l cmd.exe
- B. netcat -p 2020 -cmd.exe
- C. nc -l -p 2020 -e cmd.exe
- D. nc -p 2020 -l run/cmd.exe
- E. netcat -p 2020 -l -run cmd.exe

Answer: C

QUESTION NO: 70

In order to check on the passwords in your organization, you have been given the authority to run a password checking tool. You are going to use the tool LCP to check the passwords. What are the three main options available to you to configure LCP to attack and check passwords?

- A. Reverse Attack
- B. Dictionary Attack
- C. Hybrid Attack
- D. Brute Force Attack
- E. Cryptographic Attack

Answer: B,C,D

QUESTION NO: 71

To increase the security of your corporate website, you are running some basic checks on leaked information. You view the source code for a web page and see the following:

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<meta name="GENERATOR" content="FrontPage 4.0">
<meta name="ProgId" content="Editor.Document">
<title>Security Certifications for the IT Pro</title>
<style type="text/css">
<!--
P, TD, LI, TH { font-size: 10pt; font-family: Arial, Verdana, Helvetica }
.eight { font-size: 8pt }
-->
</style>
</head>
```

From this code, which of the following would an attacker most likely assume is the operating

system that was used to create this web site?

- A. OpenBSD
- B. FreeBSD
- C. Linux 5.0
- D. Linux 6.0
- E. Windows NT

Answer: E

QUESTION NO: 72

You read on a security website that hackers are reading Newsgroup messages to try to identify potential targets and target details. You had previously not closed the port for the Newsgroup service on your firewall.

After you close that port, you do an Internet newsgroup search for your domain name. You do find several messages from users in your organization. What type of information may be found by examining these messages?

- A. Email Address
- B. Internal Server Names
- C. Corporate Public IP Address
- D. Client Newsreader Program
- E. Client Email Program

Answer: A,C,D

QUESTION NO: 73

In your network, you have built a single domain of only Windows computers. There are 55 XP machines and 10 Windows Server 2003 machines. You are concerned about the security of your SAM files on the Servers. Windows Server 2003 is the only Operating System on the computers, and the hard drives are all formatted with NTFS. Which of the following are issues you must be sure to address when securing the SAM file?

- A. You must be sure that no user while locally logged in to the Server can delete the SAM file.
- B. You must be sure that no user while logged in to the Server remotely can delete the SAM file.
- C. You must be sure that no user can boot to DOS and delete the SAM file from there.
- D. You must be sure that no user can install a parallel Operating System and delete the SAM file from there.

E. You must be sure to encrypt the Operating System files using the built-in EFS, so that no user may delete the SAM file from anywhere.

Answer: C,D

QUESTION NO: 74

To maintain the security of your network you routinely run several checks of the network and computers.

Often you use the built-in tools, such as netstat. If you run the following command:
netstat -e which of the following will be the result?

- A. Displays all connections and listening ports
- B. Displays Ethernet statistics
- C. Displays addresses and port numbers in numerical form
- D. Shows connections for the protocol specified
- E. Displays per-protocol statistics

Answer: B

QUESTION NO: 75

One of your users calls to state that their computer is acting unusual. You go to investigate and find there is an unauthorized program installed on this computer. You examine the network and find that this program is now on other machines in the network. It seems to be unable to move through the network on its own, and is getting sent as an email attachment. What type of program is in the network?

- A. The program is a Worm.
- B. The program is a Virus.
- C. The program is a Port scanner.
- D. The program is a Trojan Horse.
- E. The program is a Macro.

Answer: B

QUESTION NO: 76

In order to obtain public IP addresses, Internet Service Providers (ISPs) contact their upstream registry or their appropriate regional registry (an IANA subsidiary) at which of the following?

-
- A. APNIC
 - B. ARIN
 - C. RIPE NCC
 - D. IETF
 - E. IESG

Answer: A,B,C

QUESTION NO: 77

You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0.

You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement an update based on a critical Microsoft Security Bulletin?

- A. Critical Update
- B. Security Update
- C. Feature Pack
- D. Update Rollup
- E. MSB Update

Answer: B

QUESTION NO: 78

You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0.

You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement an update to fix a specific problem that addresses a critical, non-security-related bug?

- A. Critical Update
- B. Security Update
- C. Feature Pack
- D. Update Rollup
- E. MSB Update

Answer: A

QUESTION NO: 79

You have a series of new Windows Server 2003 systems, including 3 new web servers running IIS 6.0.

You are concerned about the overall security of your servers, and are checking with Microsoft for any patches or updates that you might need to apply to your systems. Which of the following would you apply if you need to implement a single update, which contains a single cumulative package that includes multiple files that are used to address a problem in your IIS Servers?

- A. Critical Update
- B. Security Update
- C. Feature Pack
- D. Update Rollup
- E. MSB Update

Answer: D

QUESTION NO: 80

You have recently installed a new Linux machine, running Apache as your web server. You are running Novell SuSe Linux, and are going to use YaST to disable some unneeded modules. In the left-hand options of YaST, which section would you choose in order to disable modules for your Apache web server?

- A. Network Services
- B. Software
- C. System
- D. Software Management
- E. Miscellaneous

Answer: A

QUESTION NO: 81

You have recently installed an Apache Web server on a SuSe Linux machine. When you return from lunch, you find that a colleague has made a few configuration changes. One thing you notice is a .htpasswd file. What is the function of this file?

- A. It is a copy of the /etc/passwd file for Web access
- B. It is a copy of the etc/shadow file for Web access

-
- C. It is a listing of all anonymous users to the Web server
 - D. It is a listing of http users and passwords for authentication
 - E. It is a database file that can be pulled remotely via a web interface to identify currently logged in users.

Answer: D

QUESTION NO: 82

Recently you found out that there has been a flood of bogus network traffic hitting your Email server.

Because of this flood, authorized users have not been able to consistently send or receive email. What is happening to your Email server?

- A. A Denial of Service Attack
- B. A Virus Attack
- C. A Worm Attack
- D. A Macro Attack
- E. A Trojan Attack

Answer: A

QUESTION NO: 83

You are concerned that email messages sent to your Outlook clients could contain customized and dangerous scripting. What can you do to minimize the threat that this specific type of email presents?

- A. Install and Update Anti-Virus software
- B. Update the Security Settings for the clients at the SMTP Server
- C. Disable the Preview Pane
- D. Be sure that all forms of scripting are disabled on all clients
- E. Minimize the number of contacts allowed in an address book

Answer: C

QUESTION NO: 84

You are conducting a security awareness session for some of the employees in your organization. The discussion moves to the use of the web browser, which is Internet Explorer 7.0 for all employees. What are the four Zones that are available in Internet Explorer 7.0?

-
- A. Internet
 - B. Local intranet
 - C. Trusted sites
 - D. Restricted sites
 - E. Unrestricted sites

Answer: A,B,C,D

QUESTION NO: 85

Microsoft has developed several security tools to help you with the security and configuration of the systems in your network. One of these tools is the Microsoft Security Baseline Analyzer (MBSA). In the command line options of the MBSA is the HFNetChk tool. What is the function of the HFNetChk tool, available with MBSA?

- A. To check for the current Hotfixes that are available from Microsoft
- B. It is an upgrade to the Windows Update tool for checking on all updates
- C. It is the tool that must be run prior to installing IIS 6.0
- D. It is the tool that checks the network configuration of all web servers
- E. To record what Hotfixes and service packs are running on the Windows machine

Answer: E

QUESTION NO: 86

You just installed a new SuSe Linux web server, running Apache, and are in the process of hardening the server. The server will perform basic web services, static web pages to internal clients only. Which of the following would you not perform to harden this system?

- A. Disable server-side includes
- B. Disable CGI execution
- C. Disable httpd.conf
- D. Disable directory browsing
- E. Disable unnecessary modules

Answer: C

QUESTION NO: 87

One of the major benefits to the design of the Internet is the redundancy that is built-in. To provide a measure of fault tolerance for DNS on the Internet, the designers of the Domain Name System distributed the root servers in various countries around the world. If an attacker were to attempt to

disable DNS, they would have to gain administrative access on all the root servers. How many DNS servers would have to be compromised to have complete control of the Internet DNS?

- A. 4
- B. 8
- C. 10
- D. 12
- E. 13

Answer: E

QUESTION NO: 88

You are studying the current attack methods and find that one of your servers is vulnerable to a Buffer

Overflow attack. Which of the following do Buffer Overflows exploit?

- A. Ramdrives
- B. A program that does not do bounds checking
- C. Memory leaks in the hardware
- D. A program allowing itself to be copied
- E. Paging of memory to a disk

Answer: B

QUESTION NO: 89

Which of the following is the name of the Active X authentication system Microsoft has included to prevent Active X controls from being altered or corrupted by attackers wanting to perform unwarranted operations?

- A. Driver Signing
- B. Authenticode
- C. Certificate services
- D. NTLM
- E. Kerberos

Answer: B

QUESTION NO: 90

You work for a medium sized ISP and there have been several attacks of the DNS configuration recently.

You are particularly concerned with DNS Spoofing attacks. If an attacker is able to send out false data to a

DNS client before the response from the DNS server arrives, this is which type of DNS Spoofing?

- A. DNS Server Compromise
- B. DNS Cache Poisoning
- C. Spoofing the DNS Response
- D. DNS Source-Router Spoof
- E. IXFR Source-Spoof

Answer: C

QUESTION NO: 91

You work for a medium sized ISP and there have been several attacks of the DNS configuration recently.

You are particularly concerned with DNS Spoofing and other DNS attacks. If an attacker is able to take advantage of a BIND vulnerability to gain root access, this is which type of DNS Attack?

- A. DNS Server Compromise
- B. DNS Cache Poisoning
- C. Spoofing the DNS Response
- D. DNS Source-Router Spoof
- E. IXFR Source-Spoof

Answer: A

QUESTION NO: 92

In your organization, the majority of employees use Microsoft Outlook Express as their email client. You are configuring these systems so that applications on the employee systems cannot send email, posing as the user of the system. Under the Security tab, which option will you select to achieve this goal?

- A. Do not allow other applications to send mail as me.
- B. Disable application mail delivery.
- C. Prompt me prior to application mail delivery.
- D. Warn me when other applications try to send mail as me.
- E. Do not allow applications that could potentially transmit a virus to send mail as me.

Answer: D

QUESTION NO: 93

The Root-Level DNS servers have come under many attacks over the years. Due to attacks, such as the DDoS attack on the Root-Level DNS servers in October of 2002, which of the following systems was implemented to increase the security of the DNS servers for the Internet?

- A. Multicasting
- B. Unicasting
- C. Anycasting
- D. Broadcasting
- E. X-Casting

Answer: C

QUESTION NO: 94

Most companies that do business via the Web offer a shopping cart so you can specify all the items you want before placing the order. Poor shopping cart design, however, can allow a different kind of hack. Take a look at the HTML code sample presented here and determine the line that presents the vulnerability:

```
<FORM ACTION="http://10.0.10.236/cgi-bin/orders.pl" method="post">
<input type=hidden name="price" value="39.95">
<input type=hidden name="item_no" value="WIDGET9">
QUANTITY: <input type=text name="quantity" size=2 maxlength=2 value=1>
</FORM>
```

- A. The line specifying the Perl script orders.pl
- B. The line specifying input type for price
- C. The line specifying input type for item number
- D. The line specifying input type for quantity
- E. The line specifying input type for item number and quantity

Answer: B

QUESTION NO: 95

You have been hired to work in the security division of a global Tier One ISP. You have been given a staff of 25 people all new to network security. You wish to bring them all up to speed on the components of the Internet and how they interact. Which one of the following is not a major

component of the Internet?

- A. The Backbone
- B. NAPs (Network Access Points)
- C. ISPs (Internet Service Providers)
- D. NICs (Network Information Centers)
- E. DNS (Domain Name Service)

Answer: D

QUESTION NO: 96

You are discussing the design and infrastructure of the Internet with several colleagues when a disagreement begins over the actual function of the Tier System in the Internet's design. What is the function of the Tier System in the physical structure of the Internet?

- A. The Tier System provides the physical network with communication channels for the Internet and voice/data applications.
- B. The Tier System provides a national interconnection of systems, called peering centers, to the NAPs.
- C. The Tier System provides for a layered/hierarchical connection system of ISPs connecting to the backbone.
- D. The Tier System provides for a connection point between an ISP and the backbone of the Internet.
- E. The Tier System provides the actual connection point between a local user and the Internet.

Answer: C

QUESTION NO: 97

After a year as a senior network administrator, you have been promoted to work in the security department of a large global Tier One ISP. You are to spend one month in training on security issues, concepts, and procedures. The third day in your new position, the ISP is hit with a DDoS attack from over 100,000 computers on the Internet. While the department works to manage the attack, you monitor the impact on the network. What is the impact to the ISP when hit with a DDoS such as this?

- A. The attack compromises internal IP addresses of clients.
- B. The attack denies legitimate users the ability to access legitimate resources.
- C. The attack compromises internal email addresses of clients in the network.
- D. The attack creates a loop of data, where requests for resources are routed to a different location.

E. The attack will cause (due to the large number of computers involved) the IDS to crash and no longer log network activity.

Answer: B

QUESTION NO: 98

During a routine security inspection of the clients in your network, you find a program called cgiscan.c on one of the computers. You investigate the file, reading part of the contents. Using the portion of the program shown below, identify the function of the program.

```
Temp[1] = "GET /cgi-bin/phf HTTP/1.0\n\n";  
Temp[2] = "GET /cgi-bin/Count.cgi HTTP/1.0\n\n";  
Temp[3] = "GET /cgi-bin/test-cgi HTTP/1.0\n\n";  
Temp[4] = "GET /cgi-bin/php.cgi HTTP/1.0\n\n";  
Temp[5] = "GET /cgi-bin/handler HTTP/1.0\n\n";  
Temp[6] = "GET /cgi-bin/webgais HTTP/1.0\n\n";  
Temp[7] = "GET /cgi-bin/websendmail HTTP/1.0\n\n";
```

- A. The program is designed to launch the users email program.
- B. The program is designed to manage the counters on a target web server.
- C. The program is simply old temp files, and nothing of interest.
- D. The program is designed to test the functionality of the cgi email scripts that are installed on the server.
- E. The program is a vulnerability scanner

Answer: E

QUESTION NO: 99

You are monitoring the DNS traffic on your network to see what kind of zone transfer data is currently being exchanged. You wish to monitor the incremental zone transfers. You run a packet capture to gather network traffic for this project. Which kind of transfer traffic are you looking for?

- A. HOST
- B. MX
- C. CNAME
- D. IXFR
- E. PTR

Answer: D

QUESTION NO: 100

You work for a medium sized ISP and there have been several attacks of the DNS configuration recently. You are particularly concerned with DNS Spoofing attacks. You have a few older machines that define the storage of Resource Records (RR) based on the TTL of name mapping information. If an attacker sends fake mapping information to the DNS Server, with a high TTL, which type of DNS Spoofing is this?

- A. DNS Server Compromise
- B. DNS Cache Poisoning
- C. Spoofing the DNS Response
- D. DNS Source-Router Spoof
- E. IXFR Source-Spoof

Answer: B

QUESTION NO: 101

When using the 3DES encryption ($C = EK_1[DK_2[EK_1[P]]]$) , what is the function of P?

- A. P is the text before encryption
- B. P is the first encryption key
- C. P is the second encryption key
- D. P is the decryption key
- E. P is the text after encryption

Answer: A

QUESTION NO: 102

Public Key Cryptography systems use which two of the following keys?

- A. Symmetric Key
- B. Public Key
- C. Hash Key
- D. Asymmetric Key
- E. Private Key

Answer: B,E

QUESTION NO: 103

When a computer requires an input value to begin the cryptographic process, what is this value called?

- A. F¹ Value
- B. Entropic Value
- C. RNG Value
- D. PRNG Value
- E. Seed Value

Answer: E

QUESTION NO: 104

Which of the following are asymmetric encryption algorithms?

- A. MD5
- B. RSA
- C. Diffie-Hellman
- D. 3DES
- E. AES

Answer: B,C

QUESTION NO: 105

If you wanted to use Public Key cryptography to encrypt data transmissions, which of the following ciphers could you use?

- A. Triple-DES
- B. DES
- C. Blowfish
- D. IDEA
- E. RSA

Answer: E

QUESTION NO: 106

If you had a cipher that used a unique key every time you encoded text, what would you be using?

- A. A block cipher

-
- B. A One-time pad
 - C. A stream cipher
 - D. An asymmetric cipher
 - E. A symmetric cipher

Answer: B

QUESTION NO: 107

What can be used to remove any of the frequency and statistical relationship between unencrypted and encrypted text? (Choose two)

- A. Exponentialism
- B. Differentialism
- C. Supposition
- D. Confusion
- E. Diffusion

Answer: D,E

QUESTION NO: 108

Which of the following is a block cipher?

- A. DES
- B. 3DES
- C. AES
- D. RC4
- E. GLOC

Answer: A,B,C

QUESTION NO: 109

When using DH, what keys will Bob use to send an encrypted message to Alice?

- A. Alices Public Key
- B. Alices Private Key
- C. The Session Key
- D. Bobs Public Key
- E. Bobs Private Key

Answer: A,C,E

QUESTION NO: 110

What type of encryption converts data from a variable-length to a fixed length piece of data?

- A. Asymmetric
- B. Symmetric
- C. Hash
- D. IPSec
- E. S/MIME

Answer: C

QUESTION NO: 111

Default DES implementations use a key length that is how long?

- A. 1024 bits
- B. 72 bits
- C. 56 bits
- D. 256 bits
- E. 512 bits

Answer: C

QUESTION NO: 112

When using the 3DES encryption ($C = EK_1[DK_2[EK_1[P]]]$) , what is the function of D?

- A. D is the text before encryption
- B. D is the first encryption key
- C. D is the second encryption key
- D. D is the decryption key
- E. D is the text after encryption

Answer: D

QUESTION NO: 113

Which of the following are hash algorithms?

- A. MD5
- B. SHA
- C. RSA
- D. 3DES
- E. AES

Answer: A,B

QUESTION NO: 114

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: 115

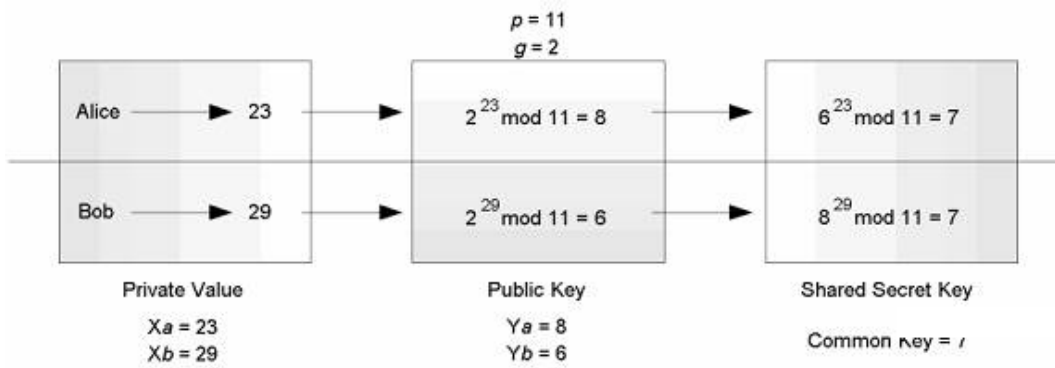
What type of cipher is used by an algorithm that encrypts data in chunks of data, 64 bits at a time?

- A. 64-bit encryption Cipher
- B. Block Cipher
- C. Stream Cipher
- D. Diffuse Cipher
- E. Split Cipher

Answer: B

QUESTION NO: 116

The image shows an example of what algorithm?



- A. DES
- B. Triple-DES
- C. Blowfish
- D. DH
- E. IDEA

Answer: D

QUESTION NO: 117

Which of the following types of attack is a vulnerability of DH?

- A. Man-in-the-middle
- B. IP Spoofing
- C. IP Sequencing
- D. Impersonation
- E. Masquerading

Answer: A

QUESTION NO: 118

When a cryptanalyst is using linguistic patterns to decrypt ciphertext, what is the analyst doing?

- A. Analyzing the frequency of letters
- B. Analyzing the degree of the letters
- C. Analyzing the Caesar Shift
- D. Analyzing the Transposition Cipher
- E. Analyzing the Substitution Cipher

Answer: A

QUESTION NO: 119

In the English language, what is the most frequently used letter?

- A. A
- B. E
- C. T
- D. R
- E. S

Answer: B

QUESTION NO: 120

When performing cryptanalysis, often the analyst will use linguistic patterns. What is a digram?

- A. A two-letter word
- B. Two letters that are next to each other in alphabetic order
- C. A two-letter combination
- D. Two letters whose letter place in the alphabet add up to an even value
- E. A three-letter combination

Answer: C

QUESTION NO: 121

What are the four different modes of implementation of DES?

- A. Stream Cycle Chaining (SCC)
- B. Electronic Codebook (ECB)
- C. Output Feedback (OFB)
- D. Cipher Feedback (CFB)
- E. Cipher Block Chaining (CBC)

Answer: B,C,D,E

QUESTION NO: 122

What type of cryptographic system is represented in this image?