Latest Version: 6

Question: 1

During a routine security inspection of the clients in your network, you find a program called cgiscan.c onone of the computers. You investigate the file, reading part of the contents. Using the portion of theprogram 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 user's 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: 2

When using multiple alphabets, what type of cipher is being used?

A. Polyalphabetic Cipher
B. Multiple Cipher
C. Multialphabetic Cipher
D. Confusion Cipher
E. Diffusion Cipher

Answer: A

Question: 3

DES is often defined as no longer "secure enough" to handle high security requirements. Why is this?

A. DES is more vulnerable to dictionary attacks than other algorithms
B. DES is more vulnerable to brute-force attacks than other algorithms
C. DES uses a 32-bit key length, which can be cracked easily
D. DES uses a 64-bit key, which can be cracked easily
E. The DES key can be cracked in a short time

Answer: E

Question: 4

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: 5

While configuring TCP Wrappers on your Linux system, you desire to create a line that will effect the single host 10.20.23.45 accessing the telnet service. Which of the following lines will achieve this desired result?

A. 10.20.23.45_HOST: in.telnetd
B. HOST(10.20.23.45): in.telnetd
C. in.telnetd: HOST_10.20.23.45
D. in.telnetd: ONLY_10.20.23.45/32
E. in.telnetd: 10.20.23.45

Answer: E

Question: 6

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: 7

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

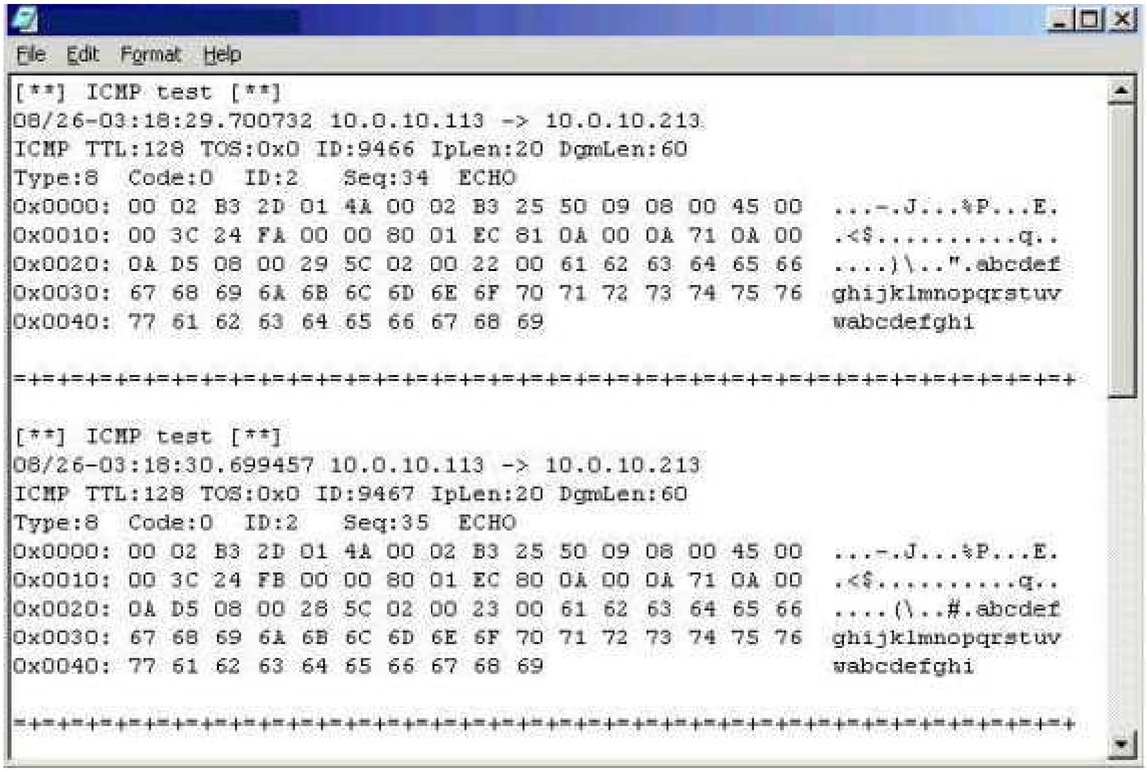
A. What are the methods available to attack this asset?
B. What are the costs associated with protecting this asset?
C. Does the threat have sufficient capability to exercise the attack?
D. Does the threat have the motivation or incentive to exercise the attack?
E. Are any of the assets worthy of an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

Answer: C, D

Question: 8

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



```
[**] ICMP test [**]
08/26-03:18:29.700732 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 [**]
08/26-03:18:30.699457 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

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

Answer: E

Question: 9

You have been given the task of writing your organization's 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: 10

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

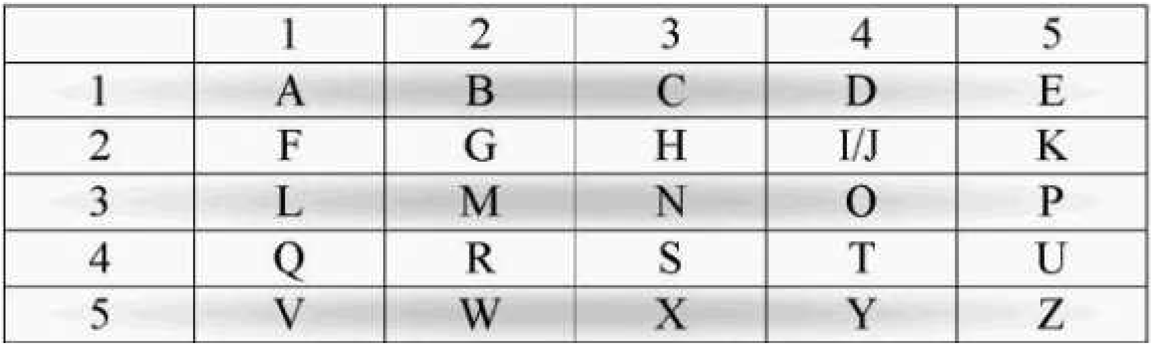
Often you use the built-in tools, such as netstat.If you run the following command, netstat -s which of the
following will be the result?

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: 11

Which of the following answers is the word SECURITY after having been encrypted using the



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A. 280
B. 34 51 31 54 24 42 44 45
C. 7 6 8 9 6 6 8 9
D. 43 15 13 45 42 24 44 54
E. 4315 4224 1345 4454

Answer: D

Question: 12

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