Free Questions for CPEH-001 by braindumpscollection

Shared by Quinn on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library. What is the name of this library?

Options:

A- NTPCAP

B- LibPCAP

C- WinPCAP

D- PCAP

Answer:

C

Explanation:

WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack, and has additional useful features, including kernel-level packet filtering, a

network statistics engine and support for remote packet capture.

Question 2

Question Type: MultipleChoice

Which of the following is NOT a valid NetWare access level?

Options:

A- Not Logged in

B- Logged in

C- Console Access

D- Administrator

Answer:

D

Explanation:

Administrator is an account not a access level.

Question 3

Question Type: MultipleChoice

What is the name of the software tool used to crack a single account on Netware Servers using a dictionary attack?

Options:

A- NPWCrack

B- NWPCrack

C- NovCrack

D- CrackNov

E- GetCrack

Answer:

B

Explanation:

NWPCrack is the software tool used to crack single accounts on Netware servers.

Question 4

Question Type: MultipleChoice

Pandora is used to attack _____ network operating systems.

Options:

A- Windows

B- UNIX

C- Linux

D- Netware

E- MAC OS

Answer:

D

Explanation:

While there are not lots of tools available to attack Netware, Pandora is one that can be used.

Question 5

Question Type: MultipleChoice

If you perform a port scan with a TCP ACK packet, what should an OPEN port return?

Options:

A- RST

B- No Reply

C- SYN/ACK

D- FIN

Open ports return RST to an ACK scan.

Answer:

A

Question 6

Question Type: MultipleChoice

If you receive a RST packet while doing an ACK scan, it indicates that the port is open.(True/False).

Options:

A- True

B- False

Answer:

A

Explanation:

When and ACK is sent to an open port, a RST is returned.

Question 7

Question Type: MultipleChoice

Which is the Novell Netware Packet signature level used to sign all packets ?

Options:

A- 0

B- 1

C- 2

D- 3

Answer:

D

Explanation:

Level 0 is no signature, Level 3 is communication using signature only.

Question 8

Question Type: **MultipleChoice**

One of the better features of NetWare is the use of packet signature that includes cryptographic signatures. The packet signature mechanism has four levels from 0 to 3.

In the list below which of the choices represent the level that forces NetWare to sign all packets?

Options:

A- 0 (zero)

B- 1

C- 2

D- 3

Answer:

D

Explanation:

0 Server does not sign packets (regardless of the client level).

1 Server signs packets if the client is capable of signing (client level is 2 or higher).

2 Server signs packets if the client is capable of signing (client level is 1 or higher).

3 Server signs packets and requires all clients to sign packets or logging in will fail.

Question 9

Question Type: MultipleChoice

Which are true statements concerning the BugBear and Pretty Park worms?

Select the best answers.

Options:

A- Both programs use email to do their work.

B- Pretty Park propagates via network shares and email

C- BugBear propagates via network shares and email

D- Pretty Park tries to connect to an IRC server to send your personal passwords.

E- Pretty Park can terminate anti-virus applications that might be running to bypass them.

Explanations: Both Pretty Park and BugBear use email to spread. Pretty Park cannot propagate via network shares, only email. BugBear propagates via network shares and email. It also terminates anti-virus applications and acts as a backdoor server for someone to get into the infected machine. Pretty Park tries to connect to an IRC server to send your personal passwords and all sorts of other information it retrieves from your PC.

Pretty Park cannot terminate anti-virus applications. However, BugBear can terminate AV software so that it can bypass them.

Answer:

A, C, D

Question 10

Question Type: MultipleChoice

You find the following entries in your web log. Each shows attempted access to either root.exe or cmd.exe. What caused this?

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..xc1x1c../..xc1x1c../..xc1x1c../winnt/system32
/cmd.exe?/c+dir
GET /scripts/..xc1x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc0xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..xc1x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

Options:

A- The Morris worm

B- The PIF virus

C- Trinoo

D- Nimda

E- Code Red

F- Ping of Death

Answer:

D

Explanation:

The Nimda worm modifies all web content files it finds. As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby, infecting the browsing system. The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines and allow intruders the ability to execute arbitrary commands within the Local System security context on machines running the unpatched versions of IIS.

Question 11

Question Type: MultipleChoice

Which of the following is one of the key features found in a worm but not seen in a virus?

Options:

A- The payload is very small, usually below 800 bytes.

B- It is self replicating without need for user intervention.

C- It does not have the ability to propagate on its own.

D- All of them cannot be detected by virus scanners.

Answer:

B

Explanation:

A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided.