GPEN$^{Q\&As}$

GIAC Certified Penetration Tester

Pass GIAC GPEN Exam with 100% Guarantee

QUESTION 1

Which of the following is the number of bits of encryption that 64-bit Wired Equivalent Privacy (WEP) effectively provides?

A. 64

B. 40

C. 60

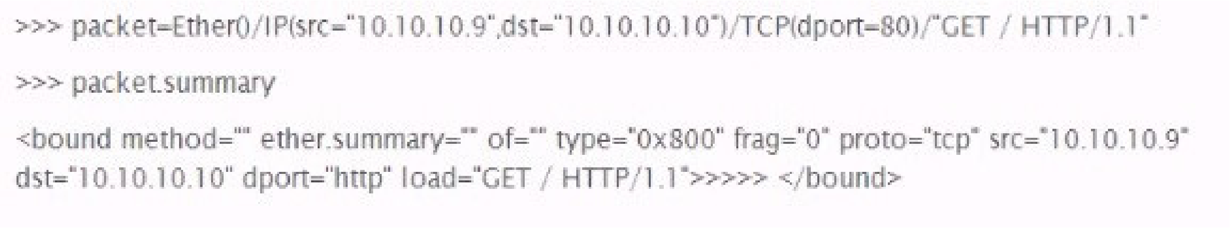
D. 44

Correct Answer: A

Reference: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

QUESTION 2

Given the following Scapy information, how is default Layer 2 information derived?



```
>>> packet=Ether()/IP(src="10.10.10.9",dst="10.10.10.10")/TCP(dport=80)/"GET / HTTP/1.1"

>>> packet.summary

<bound method="" ether.summary="" of="" type="0x800" frag="0" proto="tcp" src="10.10.10.9"
dst="10.10.10.10" dport="http" load="GET / HTTP/1.1">>>>> </bound>
```

A. The default layer 2 information is contained in a local scapy.cfg configuration fileon the local system.

B. If not explicitly defined, the Ether type field value Is created using the hex value ofthe destination port, in this case 80

C. If not explicitly defined, pseudo-random values are generated for the Layer 2 defaultinformation.

D. Scapy relies on the underlying operating system to construct Layer 2 information touse as default.

Correct Answer: D

The correct answer is D. If you actually try it, you can confirm that the MAC address adopted by scapy corresponds to the MAC address of the actual NIC.

QUESTION 3

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Man-in-the-middle

B. ARP spoofing

C. Port scanning

D. Session hijacking

Correct Answer: B

QUESTION 4

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the preattack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.

B. Map the network of We-are-secure Inc.

C. Fingerprint the services running on the we-are-secure network.

D. Install a backdoor to log in remotely on the We-are-secure server.

Correct Answer: A

QUESTION 5

Which of the following is a tool for SSH and SSL MITM attacks?

A. Ettercap

B. Cain

C. Dsniff

D. AirJack

Correct Answer: C

QUESTION 6

Adam, a malicious hacker, hides a hacking tool from a system administrator of his company by using Alternate Data Streams (ADS) feature. Which of the following statements is true in context with the above scenario?

A. Alternate Data Streams is a feature of Linux operating system.

B. Adam\\'s system runs on Microsoft Windows 98 operating system.

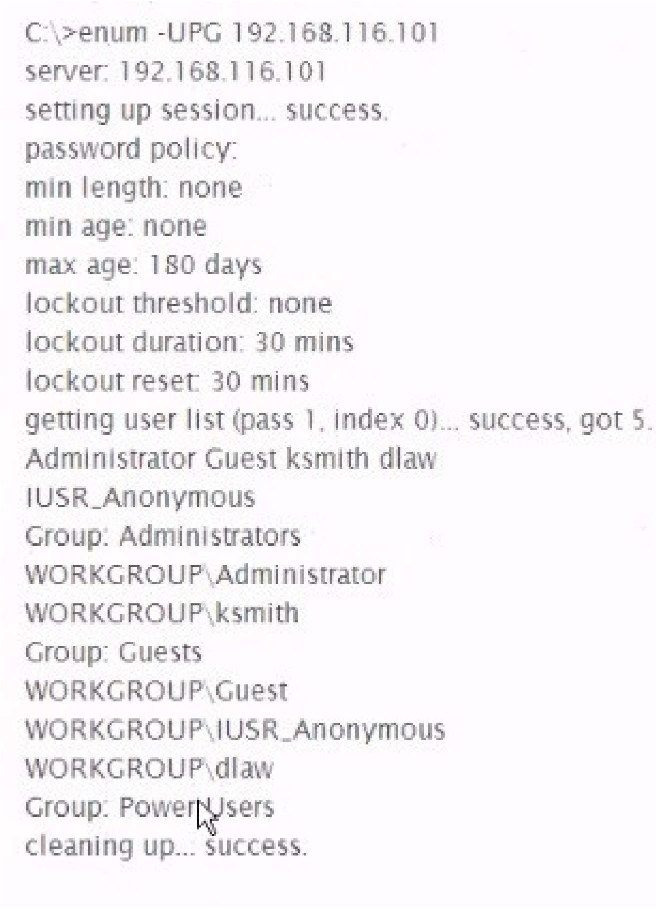
C. Adam is using FAT file system.

D. Adam is using NTFS file system.

Correct Answer: D

QUESTION 7

Analyze the command output below. What information can the tester infer directly from the information shown?



```
C:\>enum -UPG 192.168.116.101
server: 192.168.116.101
setting up session... success.
password policy:
min length: none
min age: none
max age: 180 days
lockout threshold: none
lockout duration: 30 mins
lockout reset: 30 mins
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest ksmith dlaw
IUSR_Anonymous
Group: Administrators
WORKGROUP\Administrator
WORKGROUP\ksmith
Group: Guests
WORKGROUP\Guest
WORKGROUP\IUSR_Anonymous
WORKGROUP\dlaw
Group: Power Users
cleaning up... success.
```

A. The administrator account has no password

B. Null sessions are enabled on the target

C. The target host is running Linux with Samba services

D. Account lockouts must be reset by the Administrator

Correct Answer: B

The correct answer is B. Enumerating the username and password policies of a remote machine requires a connection to IPC$, which is called Null Sessions. On the other hand, no evidence that the remote machine is Linux can be read from this image.

QUESTION 8

Which of the following techniques are NOT used to perform active OS fingerprinting? Each correct answer represents a complete solution. Choose all that apply.

A. ICMP error message quoting

B. Analyzing email headers

C. Sniffing and analyzing packets

D. Sending FIN packets to open ports on the remote system

Correct Answer: BC

QUESTION 9

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He has to ping 500 computers to find out whether these computers are connected to the server or not. Which of the following will he use to ping these computers?

A. PING

B. TRACEROUTE

C. Ping sweeping

D. NETSTAT

Correct Answer: C

QUESTION 10

Which of the following IEEE standards defines Wired Equivalent Privacy encryption scheme?

A. 802.15

B. 802.11b

C. 802.11a

D. 802.11g

Correct Answer: B

QUESTION 11

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

A. Implement WEP

B. Implement WPA

C. Don\\'t broadcast SSID

D. Implement MAC filtering

Correct Answer: C

QUESTION 12

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration.

The tool uses raw IP packets to determine the following:

What ports are open on our network systems.

What hosts are available on the network.

Identify unauthorized wireless access points.

What services (application name and version) those hosts are offering.

What operating systems (and OS versions) they are running.

What type of packet filters/firewalls are in use.

Which of the following tools is Victor using?

A. Nmap

B. Kismet

C. Sniffer

D. Nessus

Correct Answer: A

QUESTION 13

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends large number of unsolicited commercial e-mail (UCE) messages on these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail Spam

B. E-mail Storm

C. E-mail spoofing

D. E-mail bombing

Correct Answer: A

QUESTION 14

The employees of EWS Inc. require remote access to the company\\'s Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol. Which of the following statements are true about EAPTLS?

Each correct answer represents a complete solution. Choose all that apply.

A. It provides a moderate level of security.

B. It uses password hash for client authentication.

C. It uses a public key certificate for server authentication.

D. It is supported by all manufacturers of wireless LAN hardware and software.

Correct Answer: CD

QUESTION 15

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?

A. A3-07-B9-E3-BC-F9

B. F936.28A1.5BCD.DEFA

C. 1011-0011-1010-1110-1100-0001

D. 132.298.1.23

Correct Answer: A

GPEN VCE Dumps GPEN Practice Test GPEN Exam Questions