Vendor: GIAC

Exam Code: GPEN

Exam Name: GIAC Certified Intrusion Analyst

Version: DEMO

QUESTION NO: 1

You execute the following netcat command:

```
c:\target\nc -1 -p 53 -d -e cmd.exe
```

What action do you want to perform by issuing the above command?

A. Capture data on port 53 and performing banner grabbing.

B. Listen the incoming traffic on port 53 and execute the remote shell.

C. Listen the incoming data and performing port scanning.

D. Capture data on port 53 and delete the remote shell.

Answer: B

QUESTION NO: 2

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Solaris

B. Red Hat

C. Windows

D. Knoppix

Answer: C

QUESTION NO: 3

You work as a professional Ethical Hacker. You are assigned a project to perform blackhat testing on www.we-are-secure.com. You visit the office of we-are-secure.com as an air-condition mechanic. You claim that someone from the office called you saying that there is some fault in the air-conditioner of the server room. After some inquiries/arguments, the Security Administrator allows you to repair the air-conditioner of the server room.

When you get into the room, you found the server is Linux-based. You press the reboot button of the server after inserting knoppix Live CD in the CD drive of the server. Now, the server promptly boots backup into Knoppix. You mount the root partition of the server after replacing the root password in the /etc/shadow file with a known password hash and salt. Further, you copy the netcat tool on the server and install its startup files to create a reverse tunnel and move a shell to a remote server whenever the server is restarted. You simply restart the server, pull out the Knoppix Live CD from the server, and inform that the air-conditioner is working properly.

After completing this attack process, you create a security auditing report in which you mention various threats such as social engineering threat, boot from Live CD, etc. and suggest the

countermeasures to stop booting from the external media and retrieving sensitive data. Which of the following steps have you suggested to stop booting from the external media and retrieving sensitive data with regard to the above scenario?
Each correct answer represents a complete solution. Choose two.

A. Encrypting disk partitions

B. Using password protected hard drives

C. Placing BIOS password

D. Setting only the root level access for sensitive data

Answer: A,B

QUESTION NO: 4

Which of the following statements are true about KisMAC?

A. Data generated by KisMAC can also be saved in pcap format.

B. It cracks WEP and WPA keys by Rainbow attack or by dictionary attack.

C. It scans for networks passively on supported cards.

D. It is a wireless network discovery tool for Mac OS X.

Answer: A,C,D

QUESTION NO: 5

A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department. What security risk does this present?

A. An unauthorized WAP is one way for hackers to get into a network.

B. It is likely to increase network traffic and slow down network performance.

C. This circumvents network intrusion detection.

D. None, adding a wireless access point is a common task and not a security risk.

Answer: A

QUESTION NO: 6

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

Answer: B

QUESTION NO: 7

Which of the following statements are true about SSIDs?

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

A. SSIDs are case insensitive text strings and have a maximum length of 64 characters.

B. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.

C. SSID is used to identify a wireless network.

D. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

Answer: B,C,D

QUESTION NO: 8

Adam works on a Linux system. He is using Sendmail as the primary application to transmit emails.

Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination IP addresses, date and time stamps etc?

A. /log/var/logd

B. /var/log/logmail

C. /log/var/mailog

D. /var/log/mailog

Answer: D

QUESTION NO: 9

You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Answer: D

QUESTION NO: 10

Which of the following are the scanning methods used in penetration testing?

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

A. Vulnerability

B. Port

C. Network

D. Services

Answer: A,B,C