

Exam : EC-Council EC0-350

**Title : Ethical Hacking and
Countermeasures**

Version : Demo

1. You have successfully run a buffer overflow attack against a default IIS installation running on a Windows 2000

server. The server allows you to spawn a shell. In order to perform the actions you intend to do, you need elevated permissions. You need to know what your privileges are within the shell. What are your current privileges?

- A. Administrator
- B. IUSR_COMPUTERNAME
- C. LocalSystem
- D. IIS default installation account

Answer: C

2. Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Issue special cards to access secured doors at the company and provide a one-time only brief description of use of the special card
- B. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secured door
- C. Setup a mock video camera next to the special card reader adjacent to the secured door
- D. Educate all of the employees of the company on best security practices on a regular, recurring basis

Answer: D

3. Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It informs the cracker of which vulnerabilities he may be able to exploit on your system
- D. It doesn't depend on the patches that have been applied to fix existing security holes

Answer: C

4. Which of the following activities would not be considered passive footprinting?

- A. Go through the rubbish to find out any information that might have been discarded
- B. Search on financial site such as Yahoo Financial
- C. Scan the range of IP address found in their DNS database
- D. Perform multiple queries through a search engine

Answer: C

5. Bob is conducting a password assessment for one of his clients. Bob suspects that password policies are not in place and weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers. What are the means that Bob can use to get password from his client hosts and servers?

- A. Hardware, Software, and Sniffing
- B. Hardware and Software Keyloggers
- C. Passwords are always best obtained using Hardware key loggers
- D. Software only, they are the most effective

Answer: A

6. John has performed a scan of the web server with NMAP but did not gather enough information to accurately identify which operating system is running on the remote host. How could you use a web server to help in identifying the OS that is being used?

- A. Connect to the web server with a browser and look at the web page
- B. Connect to the web server with an FTP client
- C. Telnet to port 8080 on the web server and look at the default page code
- D. Telnet to an open port and grab the banner

Answer: D

7. Joseph the Hacker breaks into Hackcme Corporation's Linux system and plants a wiretap (keylogging) program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a trojan in one of the network utilities. Joseph is worried that network administrator might detect the wiretap program by querying the interfaces to see if they are running in promiscuous mode.

Running "ifconfig -a" produces the following:

```
# ifconfig -a
```

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
```

```
inet 127.0.0.1 netmask ff000000hme0:
```

```
flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,MULTICAST> mtu 1500
```

```
inet 192.0.2.99 netmask ffffff00 broadcast 134.5.2.255 ether 8:0:20:9c:a2:35
```

What can Joseph do to hide the wiretap program from being detected by ifconfig command?

- A. Block output to the console whenever the user runs ifconfig command by running screen capture utility
- B. Run the wiretap program in stealth mode from being detected by the ifconfig command
- C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information from being displayed on the console
- D. You cannot disable Promiscuous mode detection on Linux systems

Answer: C

8. Dan is conducting penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

- A. The server will send replies back to the spoofed IP address
- B. Dan cannot spoof his IP address over TCP network
- C. The scenario is incorrect as Dan can spoof his IP and get responses
- D. Dan can establish an interactive session only if he uses a NAT

Answer: A

9. What file system vulnerability does the following command take advantage of?

```
type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe
```

- A. HFS
- B. ADS
- C. XFS


```

90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..111F..1f.
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1.C.]C.]K.M.M
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1.ECf.]fE.'.M
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .E.EE...M..C
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 C..C..1?...
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 A.^u.1.F..E...
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 .M..U../bin/s
68 0a h.

```

EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)

- A. The attacker is attempting a buffer overflow attack and has succeeded
- B. The attacker is attempting an exploit that launches a command-line shell
- C. The attacker is creating a directory on the compromised machine
- D. The buffer overflow attack has been neutralized by the IDS

Answer: B

12. Which type of attack is port scanning?

- A. Web server attack
- B. Denial of service attack
- C. Unauthorized access
- D. Information gathering

Answer: D

13. What type of port scan is shown below?

Scan directed at open port:

```

Client                               Server
192.5.2.92:4079 -----FIN----->192.5.2.110:23
192.5.2.92:4079 <----NO RESPONSE-----192.5.2.110:23

```

Scan directed at closed port:

```

Client                               Server

```

192.5.2.92:4079 -----FIN----->192.5.2.110:23

192.5.2.92:4079<-----RST/ACK-----192.5.2.110:23

- A. Idle Scan
- B. Windows Scan
- C. XMAS Scan
- D. FIN Scan

Answer: D

14. Port scans are often used to profile systems before they are attacked. Knowing what ports are open allows an attacker to determine which services can be attacked.

How do you prevent a hacker from launching FIN, NULL, and X-MAS scans on your network?

- A. Modify the kernel to never send reset (RST) packets
- B. Block TCP/IP packets with FIN flag enabled at the firewall
- C. Enable IDS signatures to block these scans
- D. You cannot block a hacker from launching these scans on your network

Answer: A

15. After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server.

What attacks can you successfully launch against a server using the above technique?

- A. Session Hijacking attacks
- B. Denial of Service attacks
- C. Web page defacement attacks
- D. IP spoofing attacks

Answer: A

16. You receive an e-mail with the following text message.

Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible. You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

- A. Virus hoax
- B. Spooky Virus
- C. Stealth Virus
- D. Polymorphic Virus

Answer: A

17. Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

- A. True
- B. False

Answer: A

18. William has received a Tetris game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Tetris.

After William installs the game, he plays it for a couple of hours. The next day, William plays the Tetris game again and notices that his machine has begun to slow down. He brings up his Task Manager and sees the following programs running:

Windows Task Manager

File Options View Help

Applications Processes Performance Networking

Image Name	User Name	CPU	Mem Usage	
AcroTray.exe	Administrator	00	36 K	
Beast2.07.exe	Administrator	00	2,604 K	
csrss.exe	SYSTEM	00	3,596 K	
ctfmon.exe	Administrator	00	1,160 K	
defwatch.exe	SYSTEM	00	1,164 K	
DVDLauncher.exe	Administrator	00	56 K	
explorer.exe	Administrator	00	5,232 K	
gcasDtServ.exe	Administrator	00	8,348 K	
gcasServ.exe	Administrator	00	2,688 K	
gcasServAlert.exe	Administrator	00	4,960 K	
hkcmd.exe	Administrator	00	44 K	
Iap.exe	SYSTEM	00	1,584 K	
igfxpers.exe	Administrator	00	44 K	
issch.exe	Administrator	00	244 K	
jusched.exe	Administrator	00	28 K	
lsass.exe	SYSTEM	00	1,004 K	
MDM.EXE	SYSTEM	00	2,812 K	
mmc.exe	Administrator	00	1,380 K	
MSGSYS.EXE	SYSTEM	00	52 K	

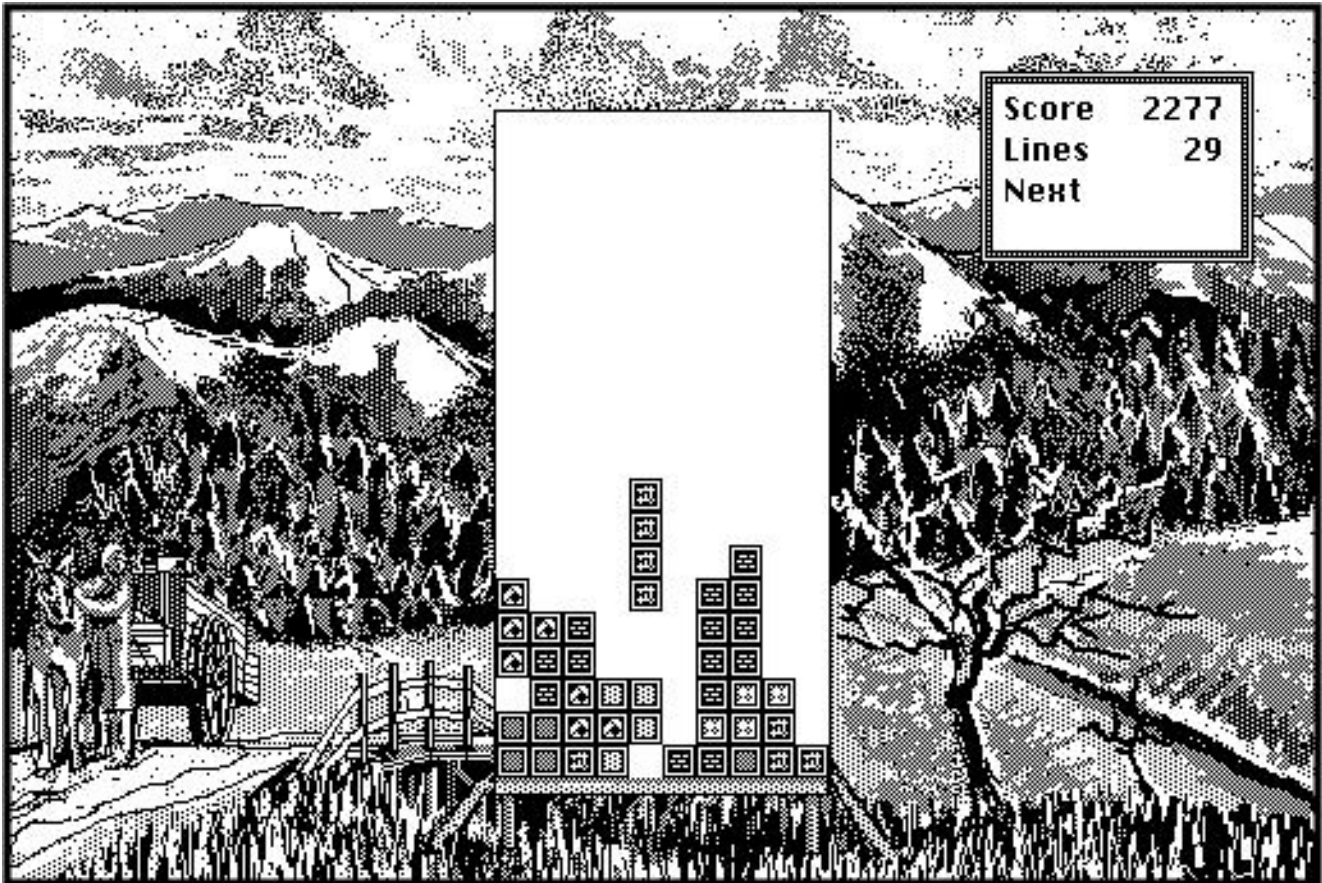
Show processes from all users

End Process

Processes: 42

CPU Usage: 4%

Commit Charge: 356M / 2445M



What has William just installed?

- A. Remote Access Trojan (RAT)
- B. Zombie Zapper (ZoZ)
- C. Bot IRC Tunnel (BIT)
- D. Root Digger (RD)

Answer: A

19. You are the security administrator for a large online auction company based out of Los Angeles. After getting your CISSP last year, you have steadily been fortifying your networks security including training, OS hardening, and network security. One of the last things you just changed for security reasons was to modify all the built-in administrator accounts on the local computers of PCs and in Active Directory. After thorough testing, you found that no services or programs were affected by the name changes.

Your company undergoes an outside security audit by a consulting company, and they said that even though all the administrator account names were changed, the accounts could still be used by a clever hacker to gain unauthorized access. You argue with the auditors and say that is not possible, so they use a tool and show you how easy it is to utilize the administrator account even though its name was changed.

What tool did the auditors use?

- A. Sid2user
- B. User2sid
- C. GetAcct
- D. Fingerprint

Answer: A

20. Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website <http://www.jeansclothesman.com>. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.

Where can Stephanie go to see past versions and pages of a website?

- A. Stephanie can go to Archive.org to see past versions of the company website
- B. She should go to the web page Samspace.org to see web pages that might no longer be on the website
- C. If Stephanie navigates to Search.com; she will see old versions of the company website
- D. AddressPast.com would have any web pages that are no longer hosted on the companys website

Answer: A