Ethical Hacking Lab Series

Lab 12: Using Armitage to Attack the Network

Certified Ethical Hacking Domains:
Introduction to Ethical Hacking,
Footprinting and Reconnaissance,
Scanning Networks,
System Hacking,
Penetration Testing

Document Version: 2013-07-18 (Beta)

Authoring Organization: Moraine Valley Community College
Written by: Jesse Varsalone

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

By the end of this lab, students will learn how to use Armitage to Attack an Internet facing Server and then pivot and attack other machines on the internal network.

This lab includes the following tasks:

- 1 – Using Armitage to Attack the Internet Facing Device
- 2 – Using Armitage to Attack a the Internal Server 2008
- 3 – Using Armitage to Attack the Internal Windows XP Machine

Domains: Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, System Hacking, Penetration Testing

Hackers can exploit weaknesses in computer systems when vulnerabilities exist. An individual responsible for the network security of a company will need to patch systems that have vulnerabilities. It is also a best practice for a network administrator to shut down any unnecessary services that are running on their systems. If systems are not maintained or properly secured, hackers can take advantage of them. After a hacker breaks into a remote system, they will take steps to entrench themselves by creating accounts, stealing credentials, and exfiltrating data from the network. By the end of this lab, the student will play the role of an attacker in which they identify and exploit a target machines. For this lab, the following terms and concepts will be of use:

Nmap – Nmap is a free program that can be used in Linux, Mac, or Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Zenmap is a GUI (or Graphical User Interface) frontend for Nmap. Nmap is available from www.nmap.org

Metasploit – Metasploit is an exploitation framework. The current version of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for the applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable, along with links to websites, which describe the exploit in more detail. To use Metasploit, you should be comfortable using the command line.

Robots.txt – This is a text file within the webroot that indicates which directories of your webserver. It indicates to web robots which directories they should traverse.

Armitage – Metasploit is a very powerful exploitation framework but it requires that the user be comfortable using the command line. Armitage is a GUI frontend for Metasploit that has many powerful capabilities. An attacker can use Armitage to identify and exploit victim machines within an easy to use graphical environment.

hashdump – One of the privileged commands that can be used within Meterpreter. It allows the attacker to dump the New Technology LAN Manager (NTLM) hashes. It will also dump the older LAN Manager (LM) hashes if they are present on the system.

Pod Topology

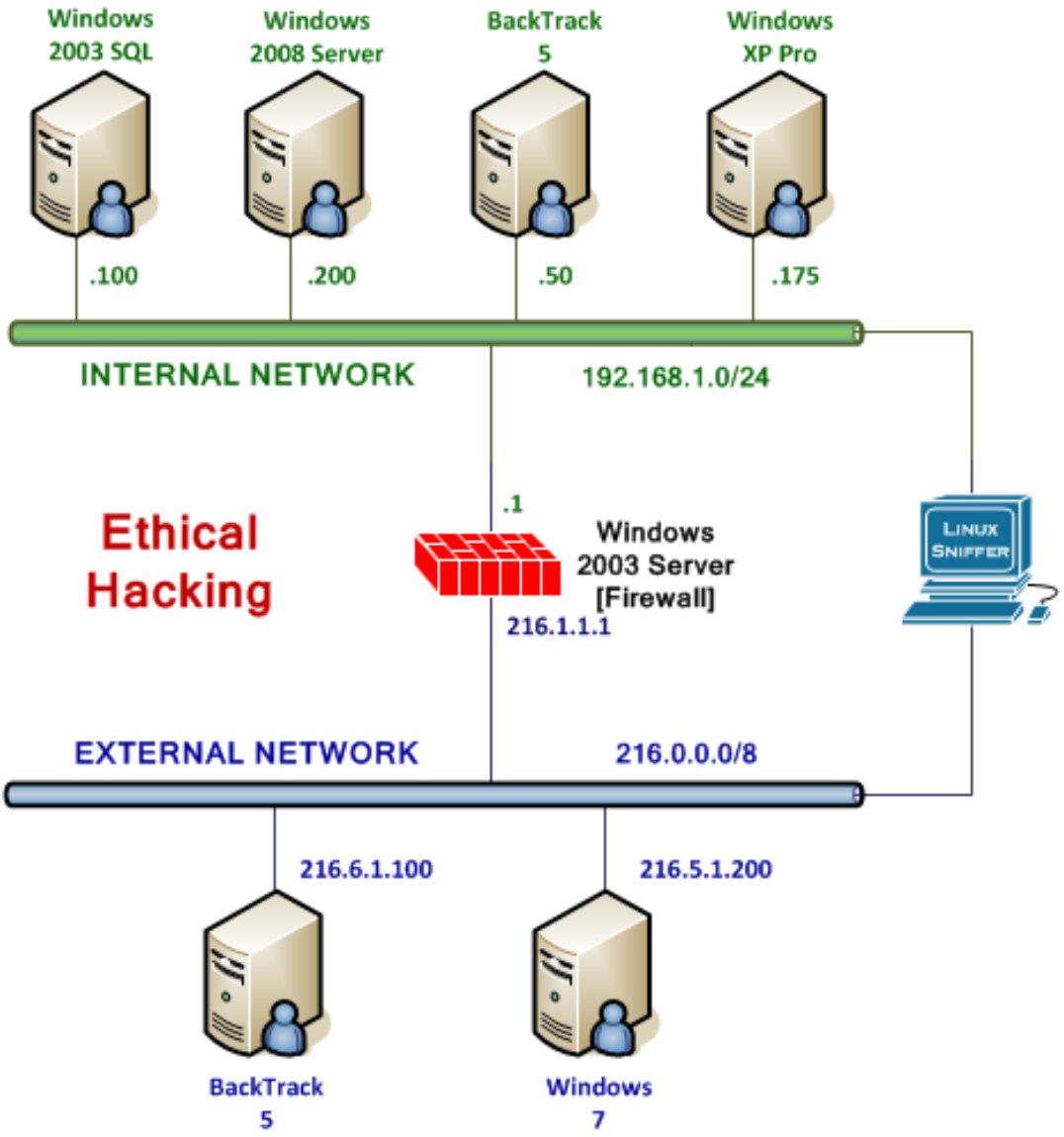


Figure 1: Lab Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

This lab requires the use of the Linux Internal Attack machine running BackTrack 5 R3 and the Windows Internal Victim Machines running Server 2003, XP and, Server 2008.

Although you will not be logging on to the Firewall, the machine is being utilized during the lab.

Windows 2008 Server	192.168.1.200
Windows 2008 Server **admin** password	none
Windows XP Pro	192.168.1.175
Windows XP Pro **Administrator** password	Ethicalhackin&
Windows 2003 SQL	192.168.1.100
Windows 2003 SQL **Administrator** password	P@ssw0rd
External **BackTrack 5**	216.6.1.100 (Public IP)
External BackTrack 5 **root** password	toor
Windows 7	216.5.1.200 (Public IP)
Windows 7 **student** password	password

1 Using Armitage to Attack the Internet Facing Device

Nmap, or network mapper, is free and runs on multiple platforms including Microsoft Windows, Mac OS X, and Linux. It can be used to determine which hosts are up on the network and then can determine which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports a remote system has running. Attackers can use Nmap to scan hosts directly on the Internet, even if they are blocking Internet Control Message Protocol (ICMP).

Never scan machines on the Internet; this lab provides a controlled environment.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Scanning the Internet Facing Device Using Nmap

1. Open a terminal on the **External BackTrack 5** Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

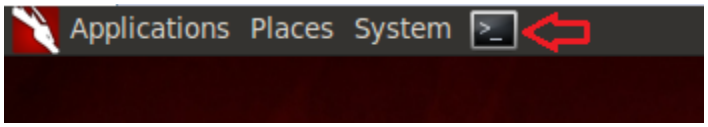


Figure 2: The Terminal Windows within BackTrack

After you click on the shortcut to the terminal, the terminal window will appear below.

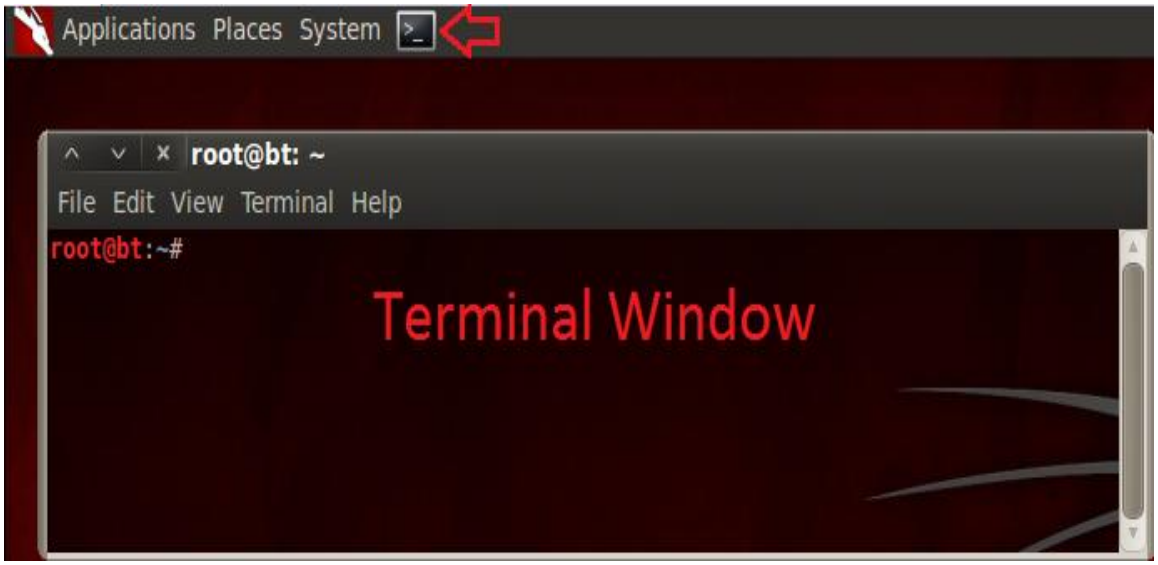


Figure 3: The BackTrack Terminal will appear

2. type the following command to open Zenmap the GUI front-end for Nmap: root@bt:~**#zenmap**

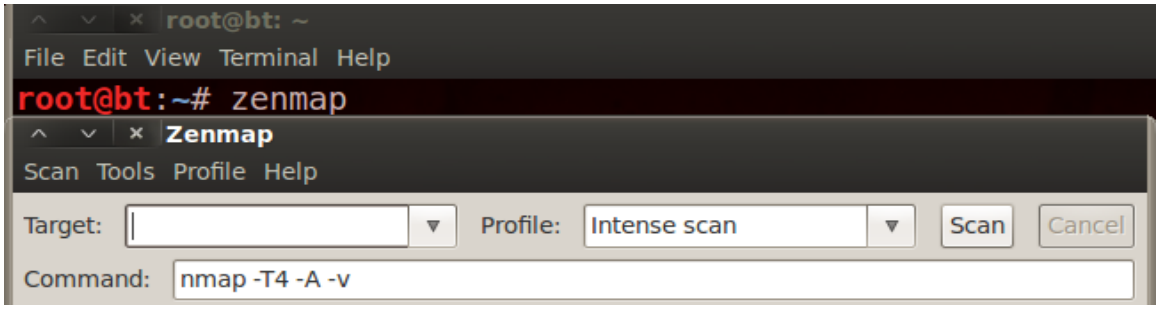


Figure 4: Open Zenmap

3. In the target box, type the Public IP address XYZcompany: **216.1.1.1**. Click **Scan**.

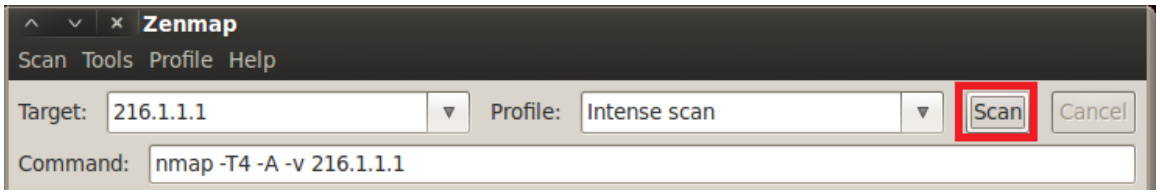
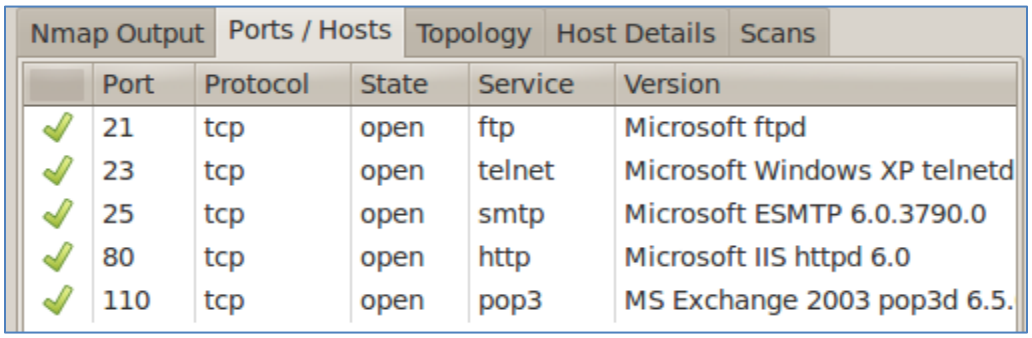


Figure 5: The Target IP

Click the **Ports/Hosts** tab. Notice that only the following 5 ports are open:

- 21 File Transfer Protocol (FTP)
- 23 TELNET
- 25 Simple Mail transfer Protocol (SMTP)
- 80 Hyper Text Transfer Protocol (HTTP)
- 110 Post Office Protocol



	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	23	tcp	open	telnet	Microsoft Windows XP telnetd
✓	25	tcp	open	smtp	Microsoft ESMTP 6.0.3790.0
✓	80	tcp	open	http	Microsoft IIS httpd 6.0
✓	110	tcp	open	pop3	MS Exchange 2003 pop3d 6.5.

Figure 6: Open Ports

4. In the Nmap Output Tab, scroll to **80/tcp**. Examine the **robots.txt** file, which restricts the directory locations that web robots can traverse.

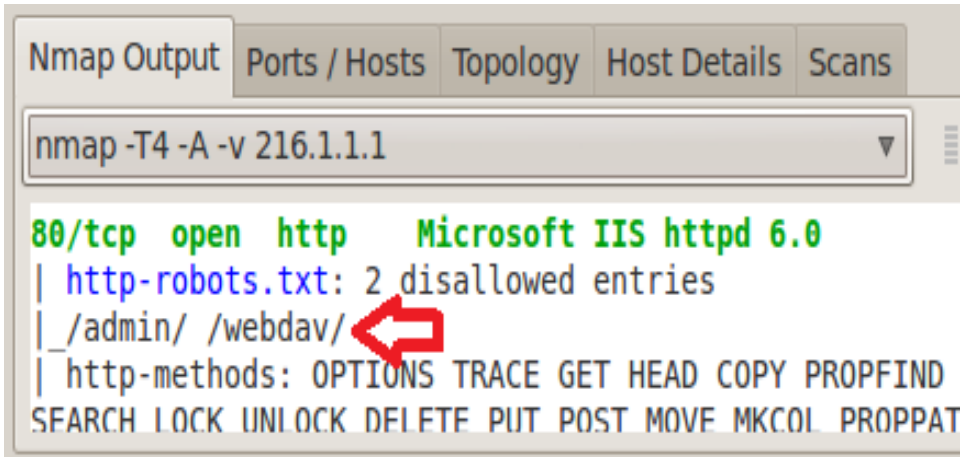


Figure 7: Information in the robotos.txt file

5. Close Zenmap. Click **No** to save changes. Type the following to launch Armitage.
` root@bt:~# **armitage**

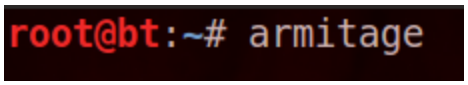


Figure 8: Launching Armitage

6. Click **Connect** to connect to the localhost as user **msf** with the password **test**.

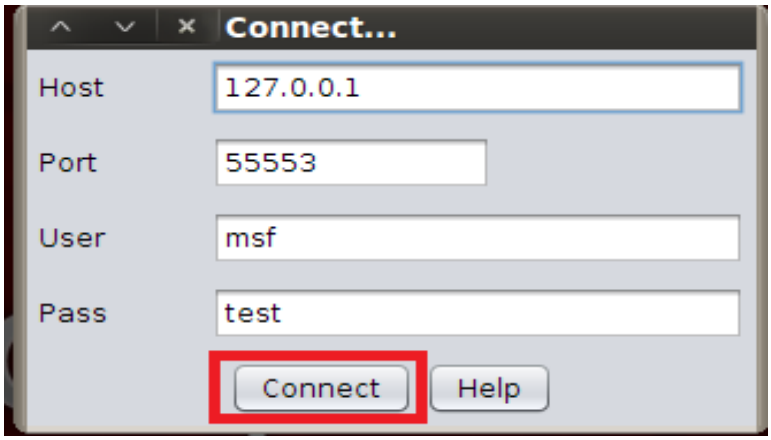


Figure 9: Connecting Armitage

7. Click **Yes** to start Metasploit's Remote Procedure Call (RPC) Server.

Figure 10: Start Metasploit RPC Server

You will initially get a java.net connection error.

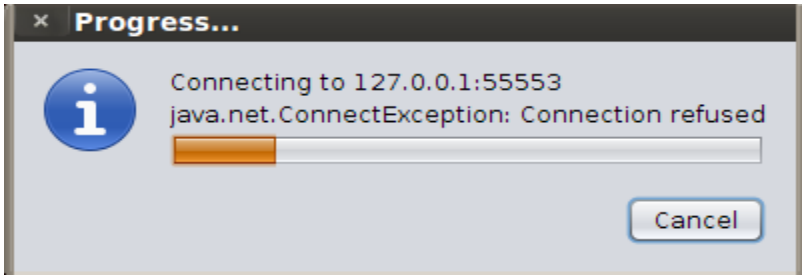


Figure 11: Java Connection Message

The Armitage windows will appear. Notice the Metasploit Console on the bottom left.

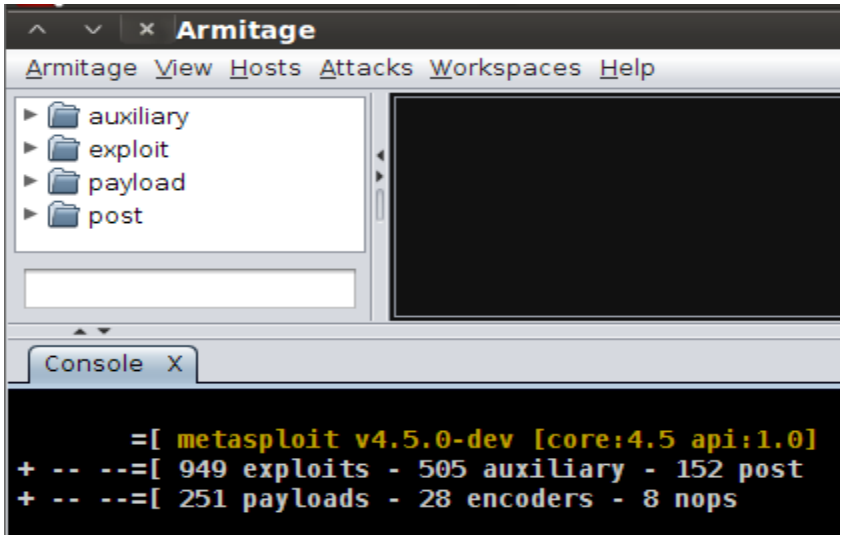


Figure 12: Armitage

8. From the Armitage menu bar, select **Hosts**, and then select **Add hosts**.

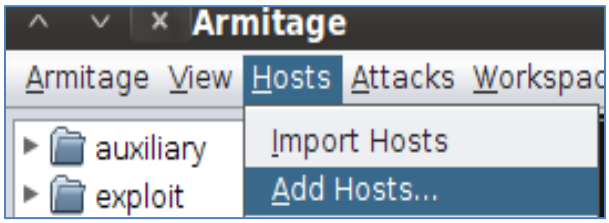


Figure 13: Adding a Host

9. In the Add Hosts box, type **216.1.1.1**, the Public IP address of XYZ Company.

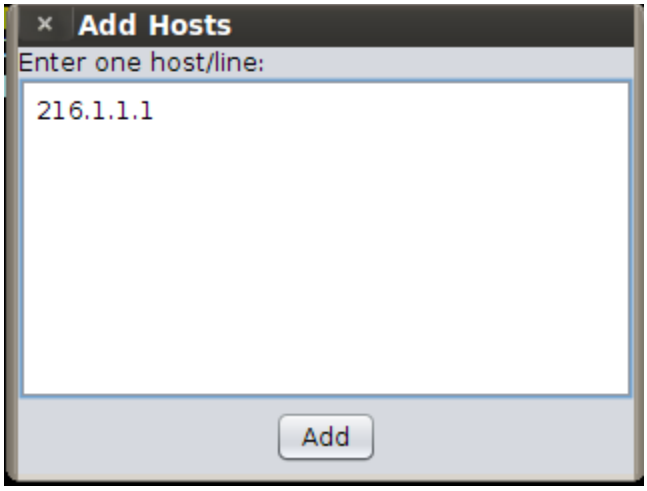


Figure 14: Adding the host 216.1.1.1

10. Click **OK** to the message box, which indicates one host was added.

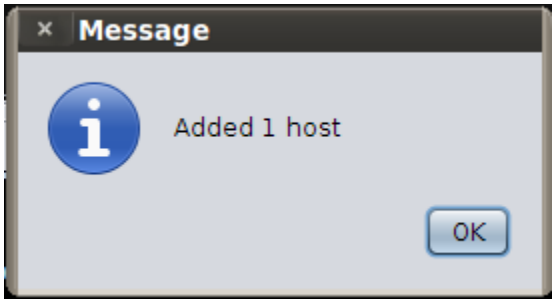


Figure 15: One Host is added

11. Right-click on host **216.1.1.1**, and select **Scan** from the list of menu choices.

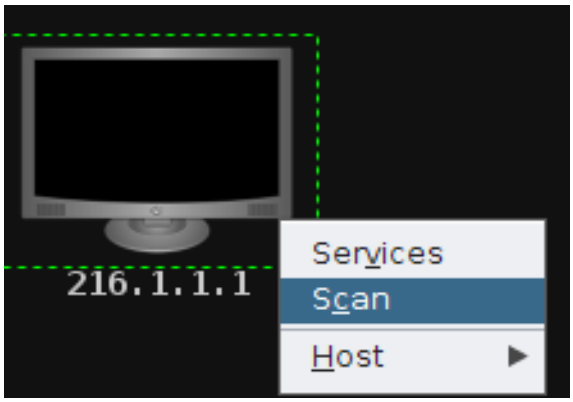


Figure 16: Scanning

The black screen changes to a Microsoft Windows emblem. The version is not identified.

Figure 17: Scanning Results

12. From the Armitage menu bar, select **Attacks** and then **Find Attacks**.

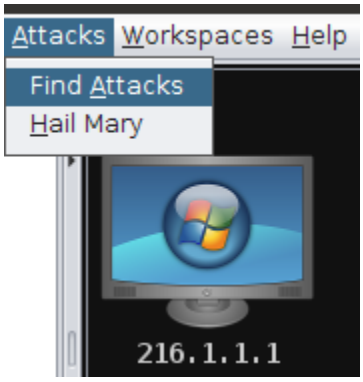


Figure 18: Finding Attacks

13. After you receive the message, *Attack Analysis Complete*, click the **OK** button.

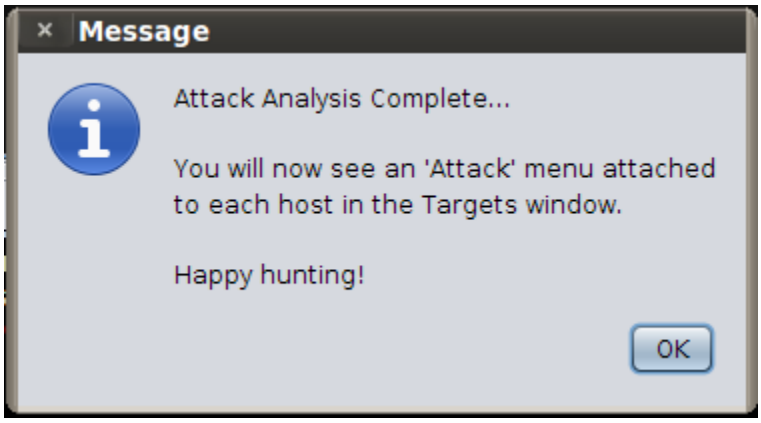


Figure 19: Finding Attacks

This is an Internet facing Windows device, so we will need to attack an Internet Information Service. Unfortunately, most of the IIS attacks work against Windows 2000 machines, and our banner messages seemed to indicate a Windows 2003 Server.

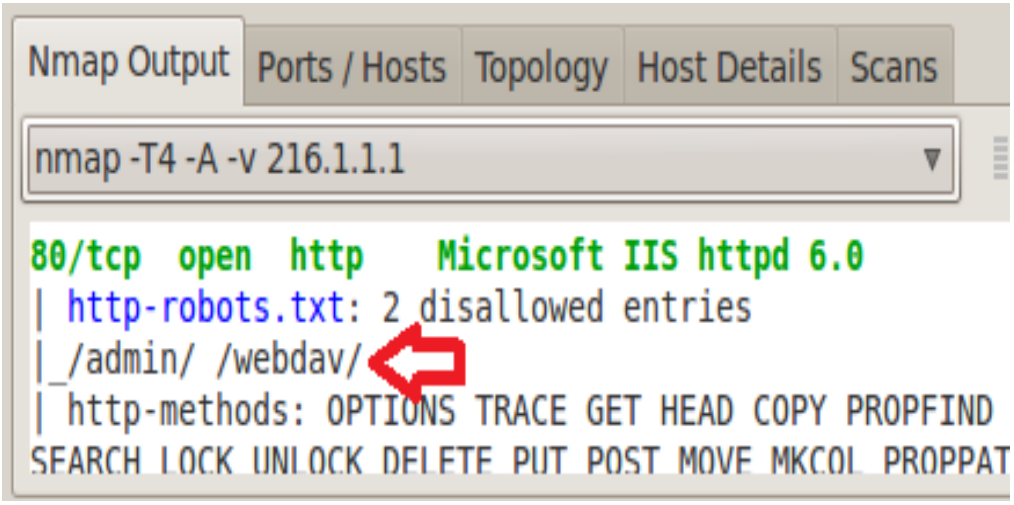


Figure 20: Finding Attacks

While most of the attacks against IIS will not work against Windows 2003, one that does work is the Web Distributed Authoring and Versioning WEBDAV attack. WEBDAV allows users to collaborate on documents using web-based authentication. While we do not know for sure that WEBDAV is enabled on this machine, we do see a folder named webdav that is mentioned in the robots.txt file, which restricts webroot access to web bots.

14. To attempt the IIS WEBDAV Attack, right-click on **216.1.1.1** and select **Attack**, then select **IIS** from the menu, and then select **iis_webdav_upload_asp**.

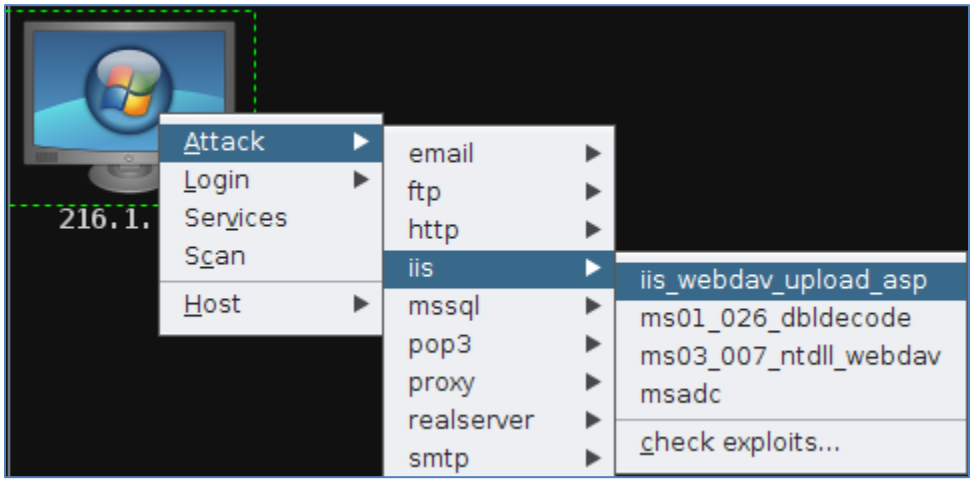


Figure 21: Selecting the WEBDAV exploit

15. Double-click in the **PATH** field and change the path to **/webdav/%RAND%.asp**. Check the box under target that states **Use a reverse connection** and click **Launch**.

Figure 22: Launching the Exploit

The target will change to red (with lightening) to indicate that it has been compromised.

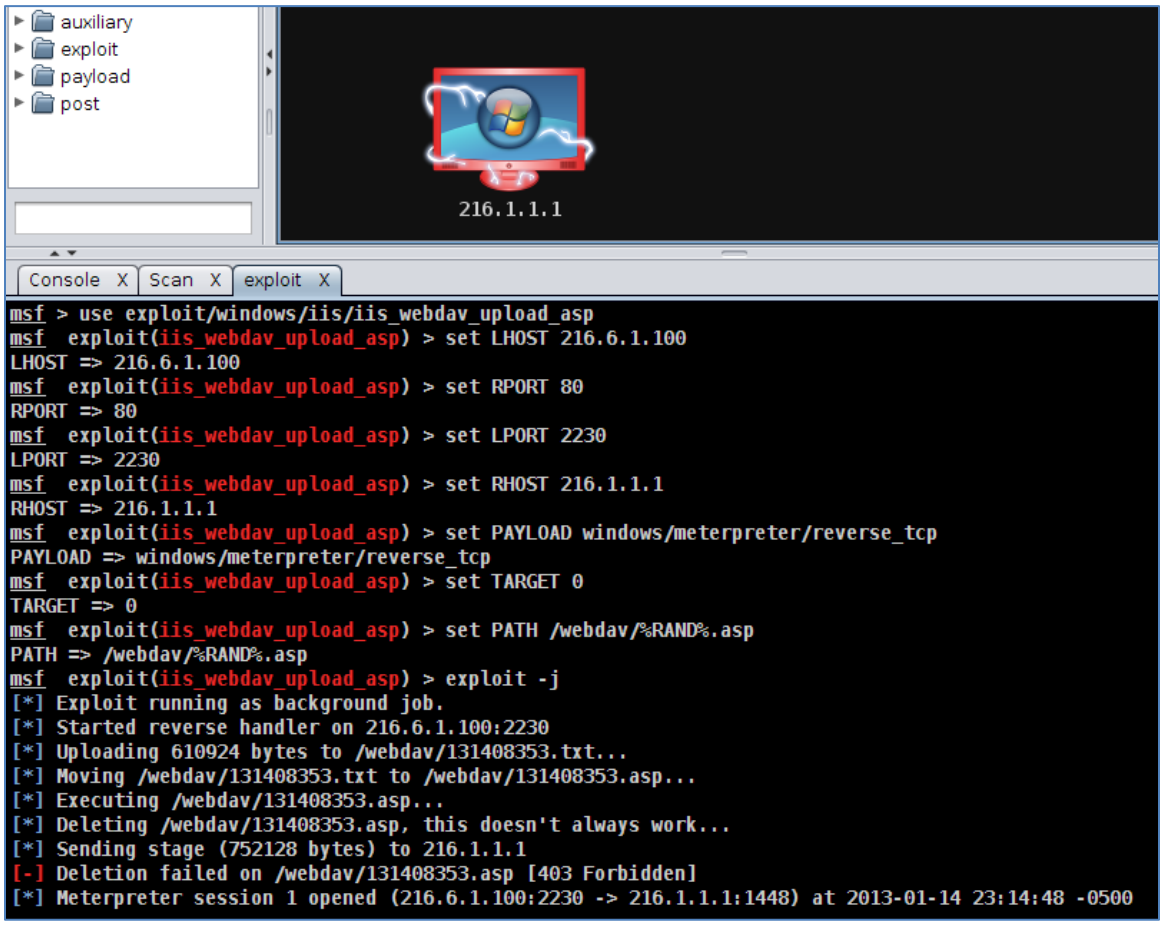


Figure 23: 216.1.1.1 is Compromised

16. Right-click on **216.1.1.1**, select **Meterpreter 1**, **interact**, and **Meterpreter Shell**.

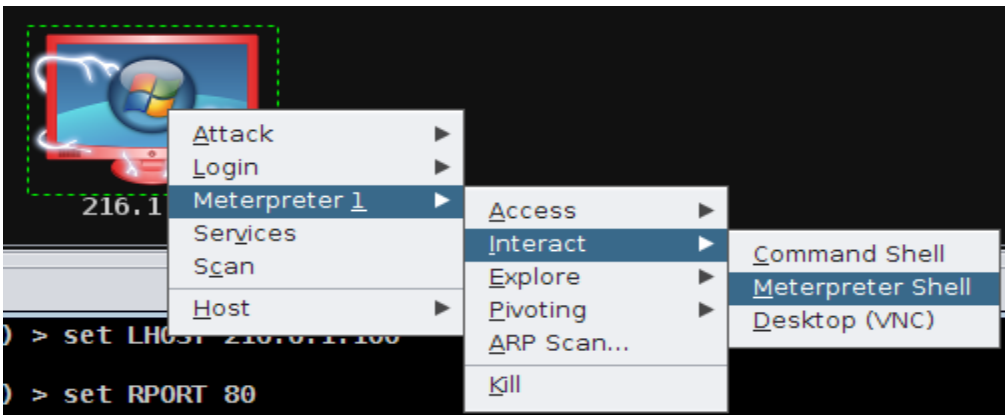


Figure 24: Interacting with Meterpreter

17. In the Meterpreter 1 below, type the following command to escalate privileges.
meterpreter > **getsystem**

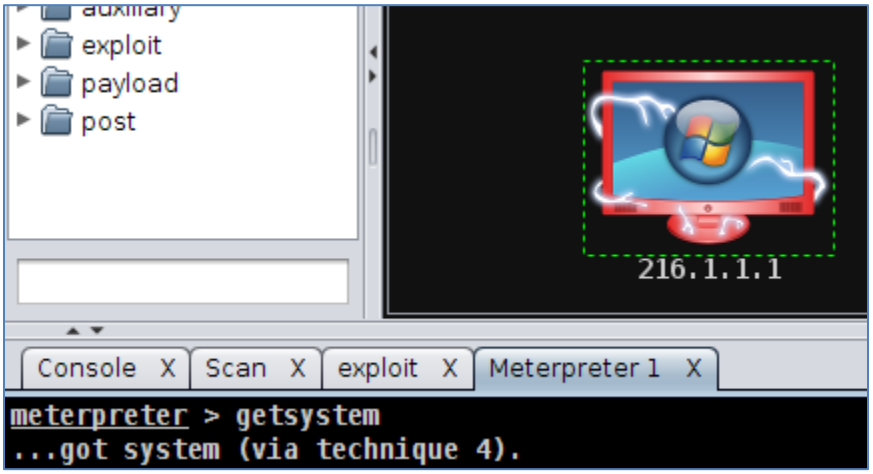


Figure 25: Escalating Privileges

1.2 Conclusion

The systems most at risk within an organization are the ones that sit directly on the Internet. A lack of patching, updating, or general misconfigurations can make those systems vulnerable. If an attacker exploits a system on a company's network with a Public IP address, it is possible that they will be able to target machines on the internal network.

1.3 Discussion Questions

1. What does the robots.txt file do?
2. What is the default protocol that uses port 21 by default?
3. What protocol has a default port of 110?
4. What is WEBDAV used for?

2 Using Armitage to Attack a the Internal Server 2008

Once an attacker gets access on the Internal Victim, they will scan for additional victims and exploit them also. Now, that the attacker is on the inside of the firewall, they can attack machines with ports like 139 and 445 open. These ports are rarely open on machines connected to the Internet but are typically open on Windows machines connected to a LAN. In this specific case, these ports are open because the administrator of the Windows 2008 server shared a single folder on the C: Drive called "share". You will typically see those ports open on Windows systems, and they are related to File and Print Sharing for Microsoft Windows. The role of this Windows 2008 server on the network is a File Server, so for that reason, those ports need to be open.

2.1 Pivoting and Attacking Server 2008

You have now entered the company XYZ network and have access to the SQL server.

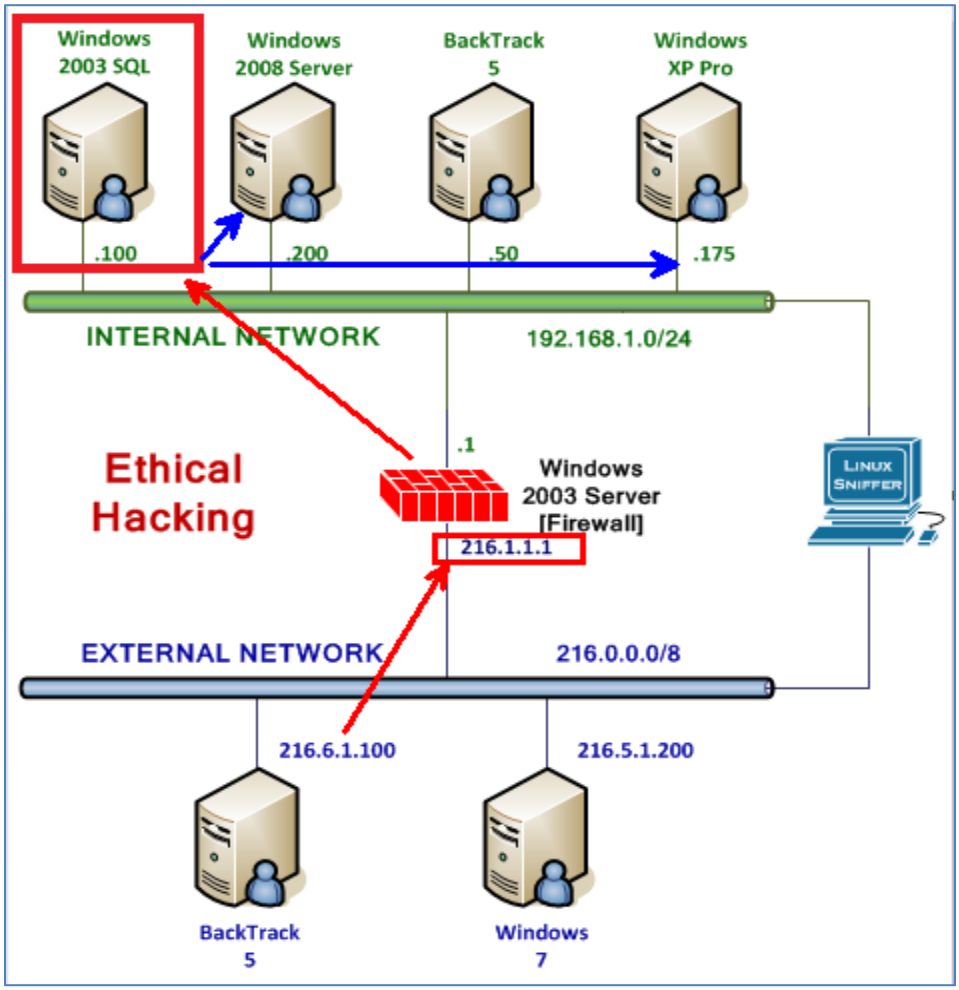


Figure 26: Internal Network

1. Right-click on the host **216.1.1.1** again. From the Armitage menu, choose **Meterpreter 1**, and select **ARP Scan**.

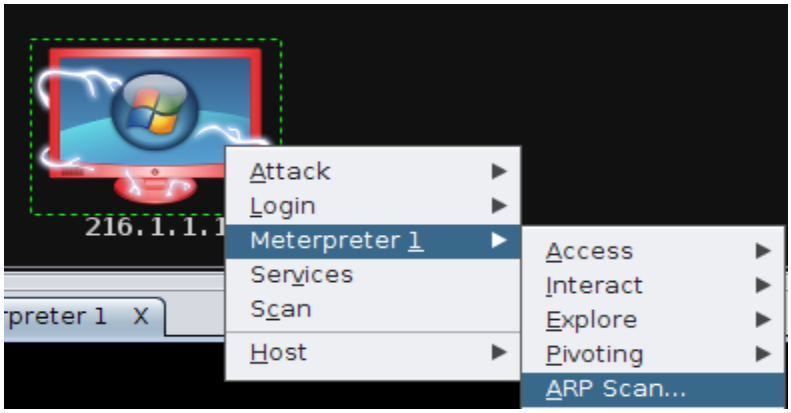


Figure 27: ARP Scan

2. From the **Armitage** menu, choose **Set Exploit Rank**, and select **Poor**.

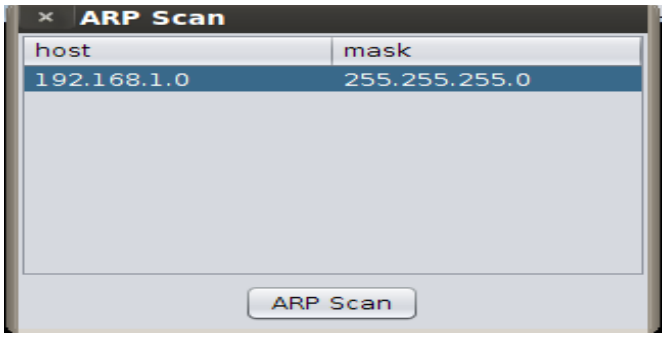


Figure 28: ARP Scan Network

All four Windows boxes should appear. If not, log into the boxes and ping the gateway of 192.168.1.1. This will simulate normal network activity if the network was in use.

Figure 29: Internal Network Layout

3. Right-click on the host **216.1.1.1**, choose **Meterpreter 1**, **Pivoting**, and **Setup**.

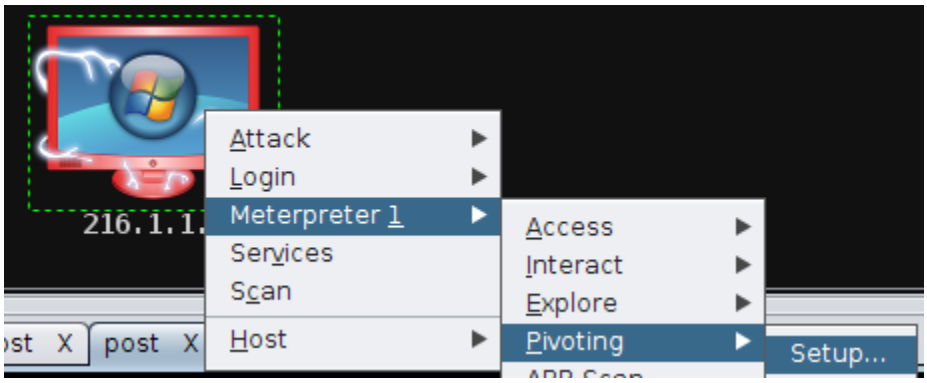


Figure 30: Setting up Pivoting

4. View the Internal Network of 192.168.1.0 and click **Add Pivot**.

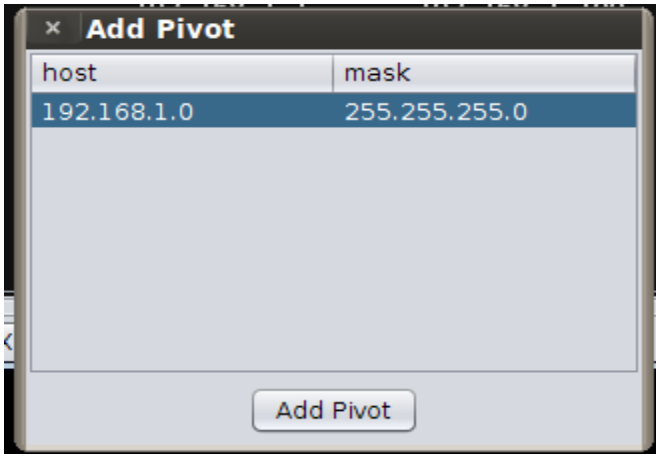


Figure 31: Adding the Pivot Route

5. Click **OK** to the message Route added

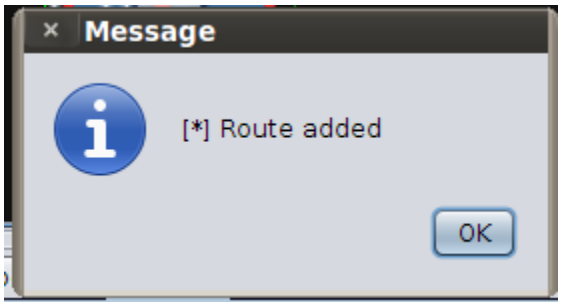


Figure 32: Route Added Message

A Green arrow will now appear connecting 216.1.1.1 to all of the Internal Victims.

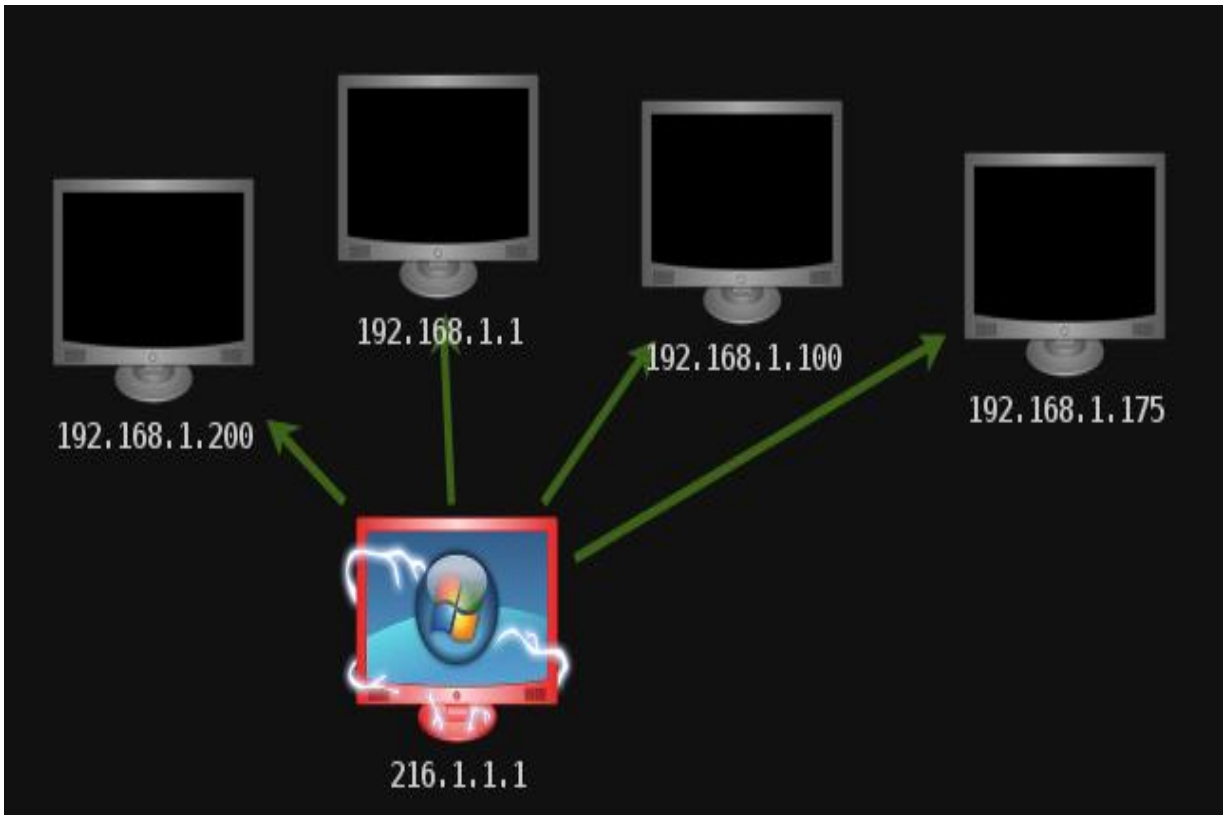


Figure 33: Green Arrow from Pivot Machine

6. Make sure the Exploit Rank is set to Poor: From the **Armitage** menu, choose **Set Exploit Rank**, and select **Poor**.

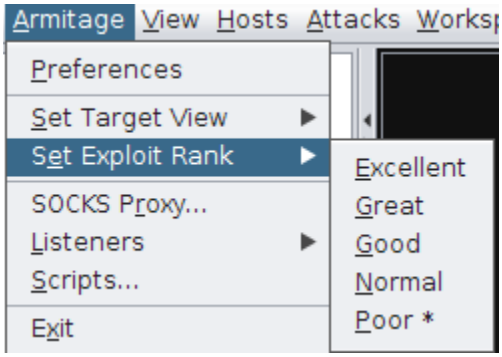


Figure 34: Lowering Exploit Rank

7. Click **OK** to the message that states, *Updated minimum exploit rank*.

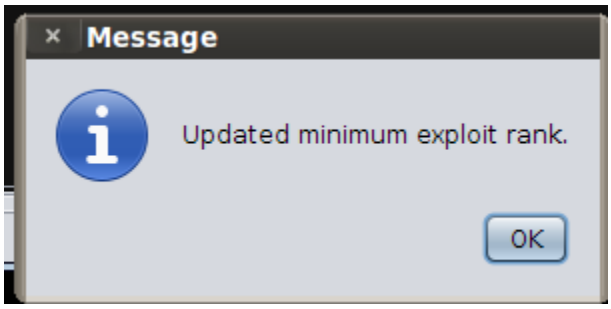


Figure 35: Minimum Exploit Rank Updated

8. Right-click on the host **192.168.1.200** in the Armitage pane and select **Scan**.

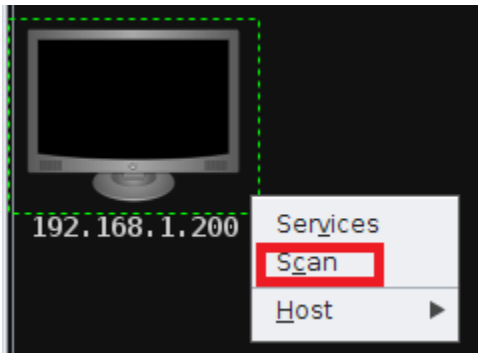


Figure 36: Scanning the Victim Machine

9. After about 5-6 minutes, your target will be identified. If you hover over the icon, the remote machine will be identified as **Windows Server 2008 Standard without Hyper-V SP1**.

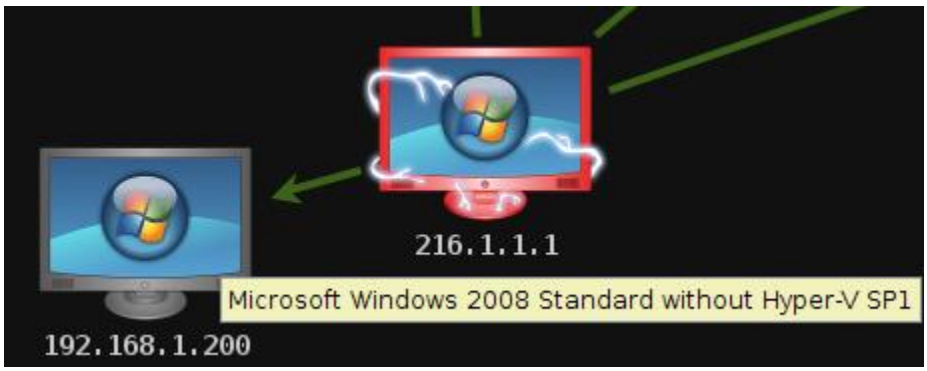


Figure 37: The Victim Machine Operating System is identified

10. From the **Attacks** menu in Armitage, select **Attacks** and then **Find Attacks**. Wait until you receive the message from Armitage that states, *Happy Hunting*.

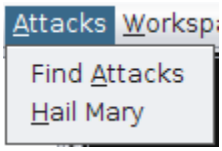


Figure 38: Finding Attacks

11. Right-click on the icon representing the victim **192.168.1.200** in the Armitage pane and select **Attack**, **smb**, **ms09_050_smb2_negotiate_func_index**

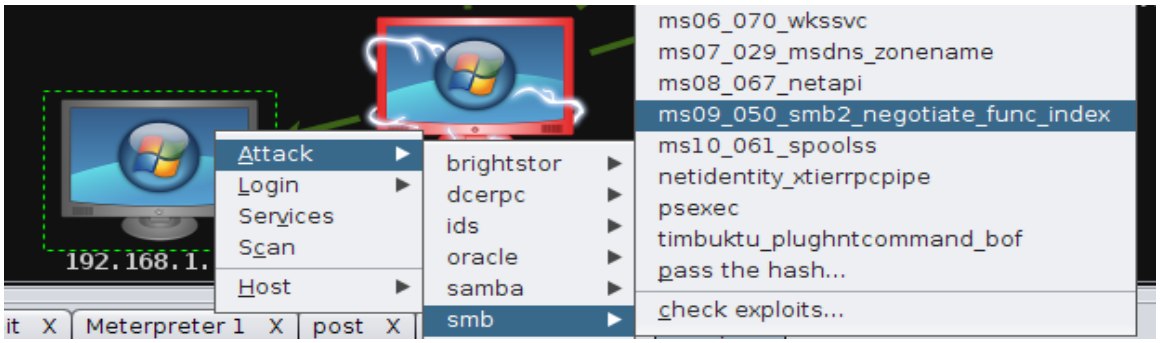


Figure 39: ms09_050_smb2_negotiate_func_index Attack

12. In the Launch Window, the title should be Attack 192.168.1.200. Check the box that says **Use a reverse connection** and then click **Launch**.

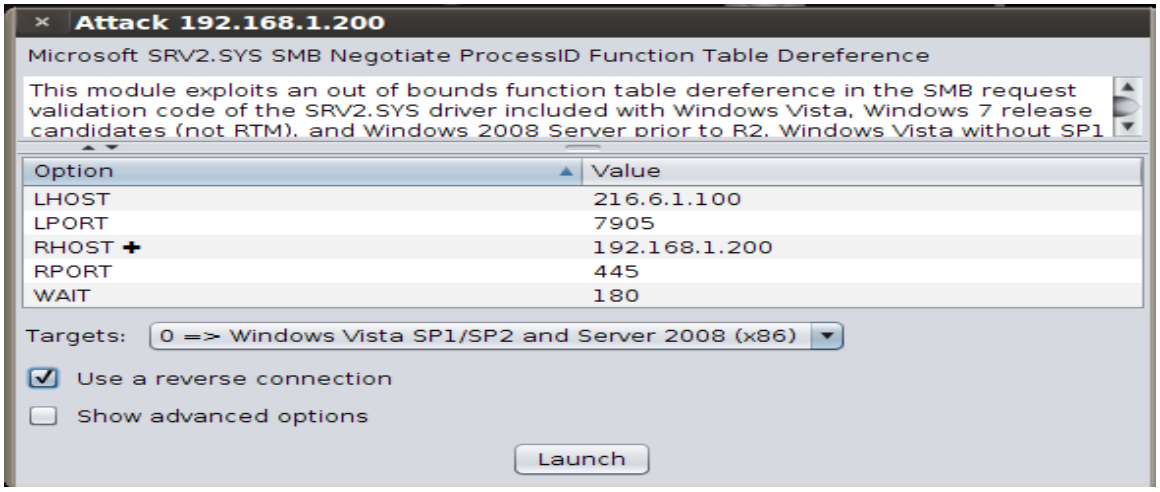


Figure 40: Launching the Attack against the Victim Machine

If the attack is successful, the victim machine will turn red. If it does not work, you may need to attempt to launch the attack again. If all else fails, reboot the **Windows 2008 Server** machine. Once the attack is successful, the victim is considered to be in a compromised state.

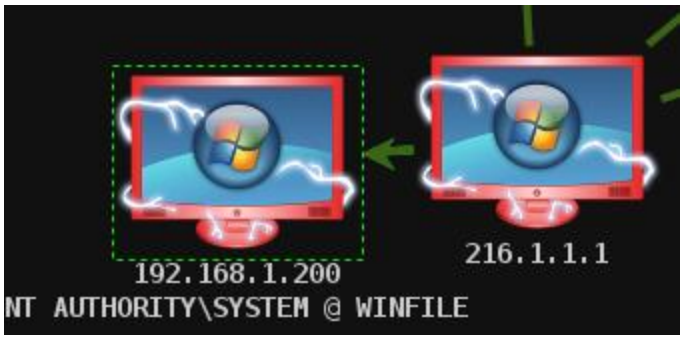


Figure 41: The Attacker is connected to the Victim Machine as SYSTEM

If the attack does not initially work, reboot the Windows 2008 Server machine. Perform steps 9 through 12 again and the exploit should work successfully. Notice that the level of access of **NT AUTHORITY\SYSTEM** is displayed by Armitage.

2.2 Conclusion

When an attacker is connected to a victim on an internal network, they can use that machine to pivot and attack other machines on the internal network with Private IP addresses. After scanning a machine, Armitage will report what operating system and service pack level the target machine is using. The Armitage tool then allows the attacker to find attacks by open ports. More ports will likely be open on machines on internal networks as opposed to machines directly connected to the Internet. If the attacker is able to connect to another victim, it will be displayed with a red border.

2.3 Discussion Questions

1. Armitage is a GUI front end for what exploitation tool?
2. How do you set up pivoting on Armitage?
3. What is pivoting?
4. What does an ARP scan do?

3 Using Armitage to Attack the Internal Windows XP Machine

Attacking the servers is always a top priority because they often store important company data or intellectual property. An attacker may often exploit workstations as well for a variety of reasons. Workstations often have looser permissions than their server counterparts and they may also be lower on the priority scale for patching and updates which would usually make them more vulnerable to attack.

3.1 Exploiting the Workstation

The attacker now has control of the **Windows 2003 SQL** and **Windows 2008 Server** machines on the internal network. The next move for the attacker is to attack the **Windows XP Pro** workstation.

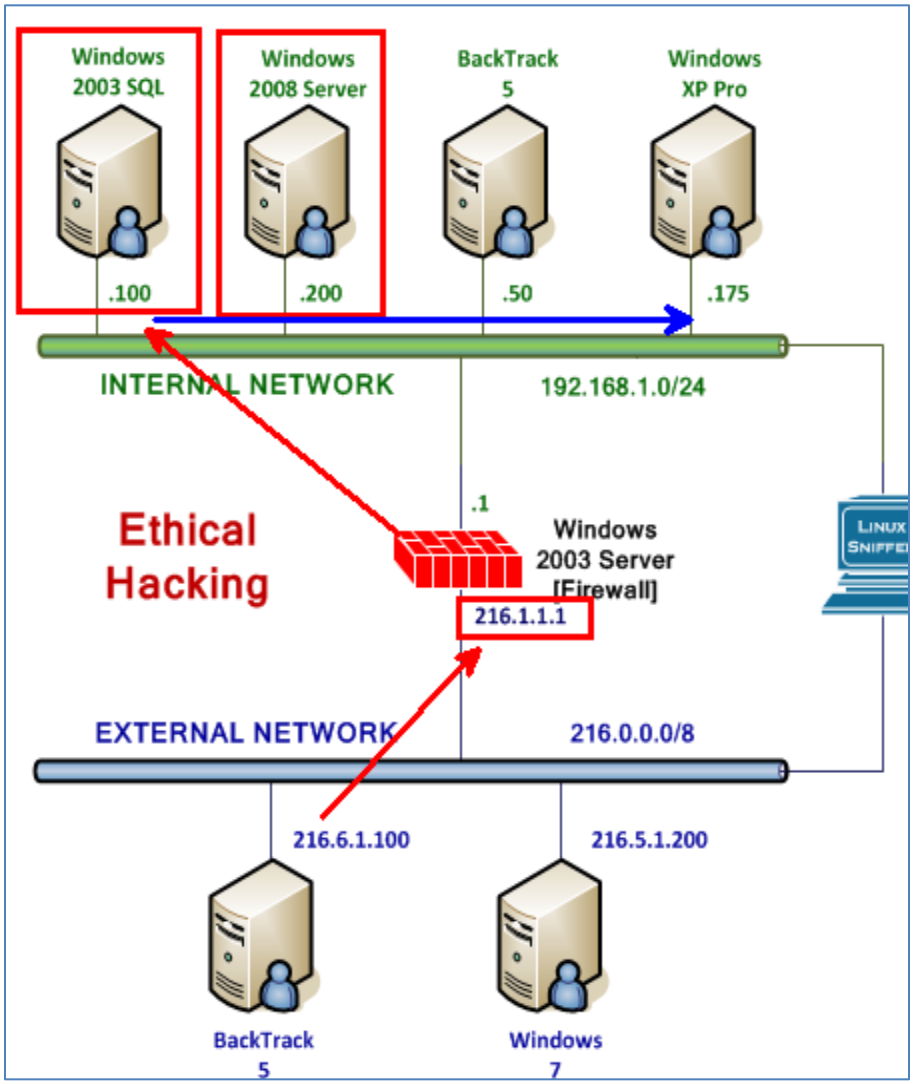


Figure 42: Internal Network Compromises

1. Instead of scanning the device, we will try a different technique. Open a command shell on the **Windows 2003 SQL** machine by selecting **Meterpreter 1 > Interact Command Shell**.

Figure 43: Interacting with a Command Shell

2. To list the available domains on the network, type the following:
c:\windows\system32\inetsrv> **net view /domain**

Figure 44: Net View

The domains on the Internal network are WORKGROUP and XYZCOMPANY.

3. To see what machines in the workgroup of WORKGROUP, type the following:
c:\windows\system32\inetsrv> **net view /domain:WORKGROUP**

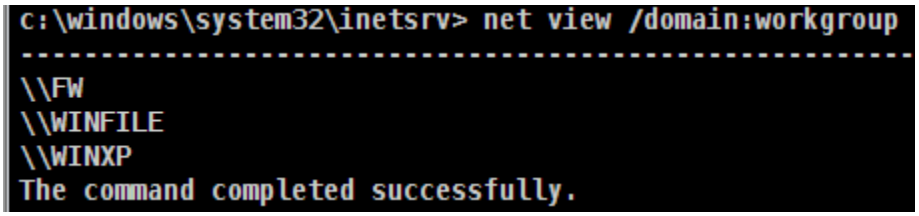


Figure 45: Net View of Workgroup Computers

It is very common for administrators to put OS names in their computer naming conventions.

4. To manually designate the operating system of the remote host, right-click on **192.168.1.175** and select **Operating system > Windows > XP/2003**.

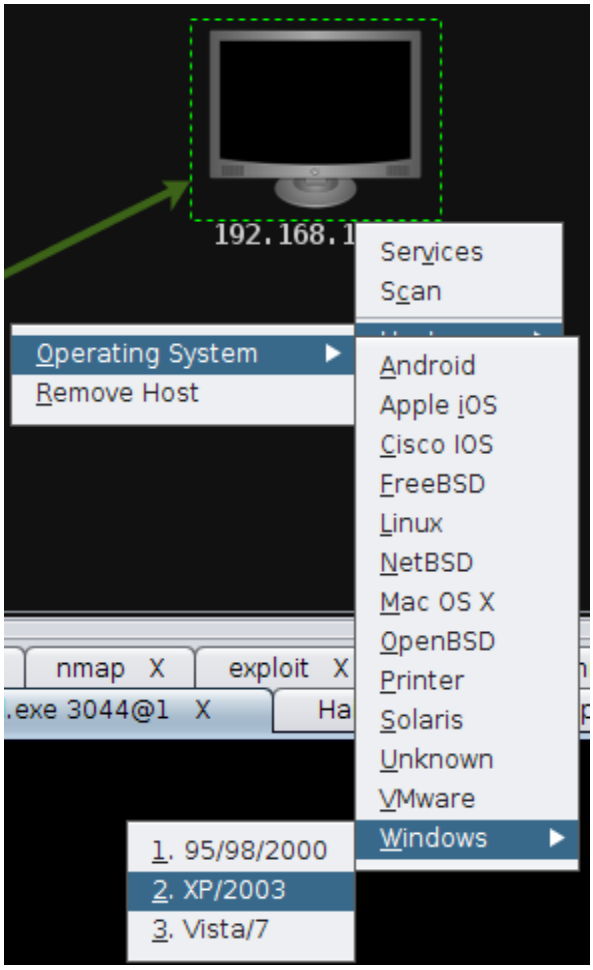


Figure 46: Manually Designation of Operating System

5. Hover over the machine with IP address **192.168.1.175** to see Windows XP.

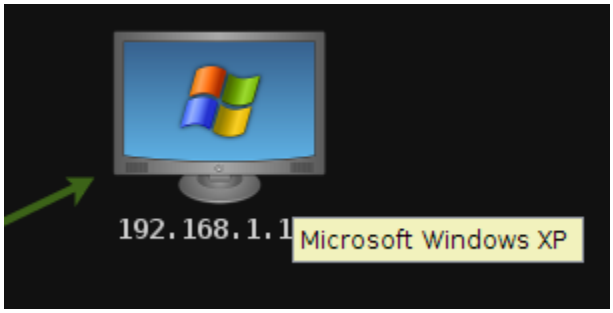


Figure 47: OS is Identified

6. Right-click on the host and select scan to scan the machine for open ports. It may take 5-6 minutes for the scan to complete.

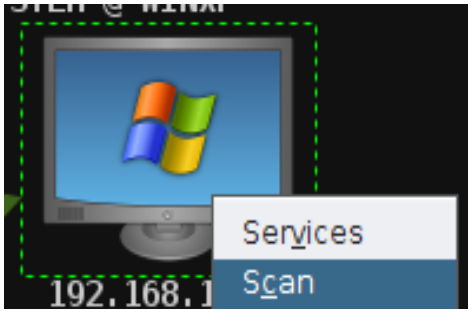


Figure 48: Scanning for Open Ports

7. From the **Attacks** menu in Armitage, select **Find Attacks**. Wait until you receive the message from Armitage that states, *Happy Hunting*.

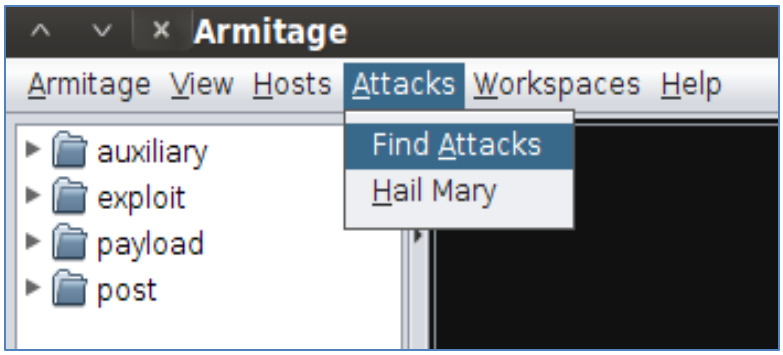


Figure 49: Finding Attacks

8. After you receive the message Attack Analysis Complete, click the **OK** button.

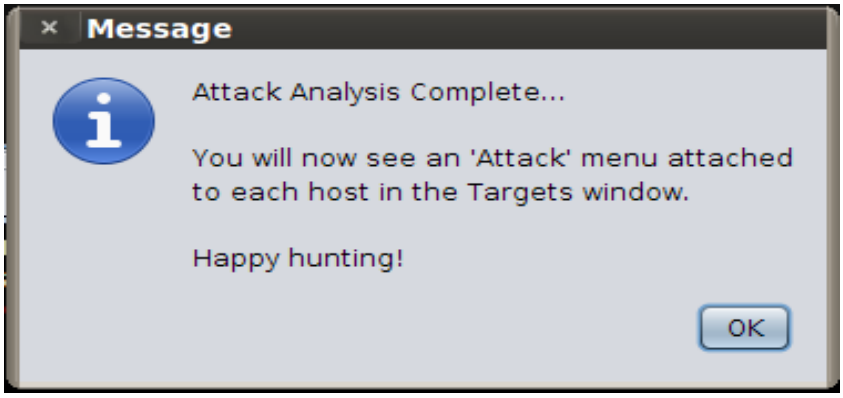


Figure 50: Finding Attacks

9. Right-click on the icon representing the victim **192.168.1.175** in the Armitage pane and select **Attack>smb>ms08_067_netapi exploit**. In the Launch Window, the title should be **Attack 192.168.1.175**. Check the box that says **Use a reverse connection** and then click **Launch**.

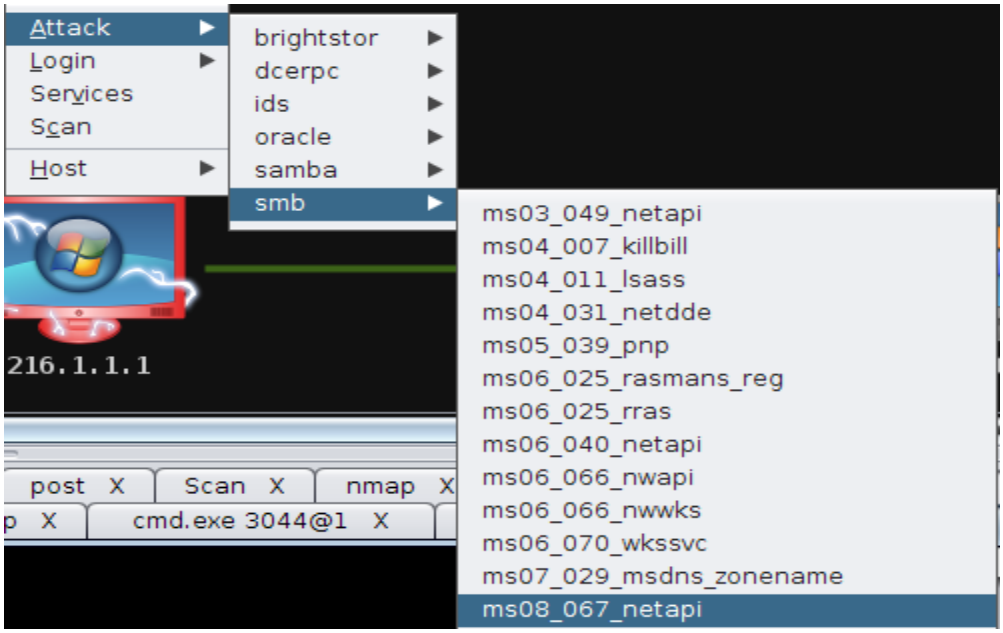


Figure 51: ms08_067_netapi Attack

You should now have 3 compromised machines on the Internal Network.

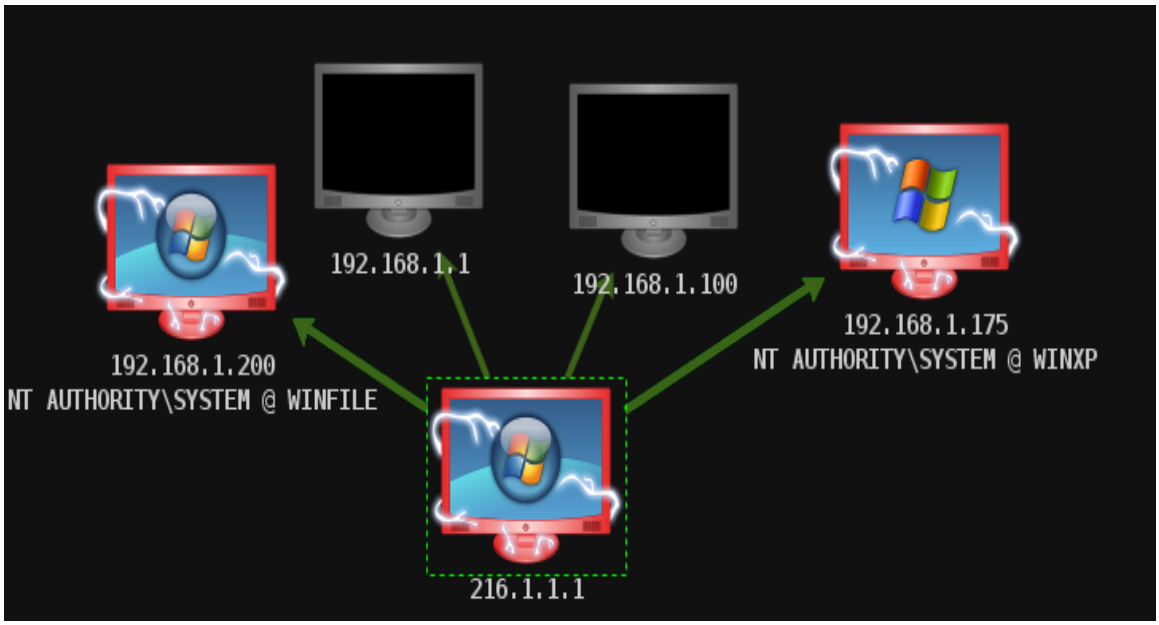


Figure 52: The Targets are exploited

You also have SYSTEM level access on all of these Microsoft Windows systems.
After gaining control of the network, the attacker can perform post exploitation tasks, such as the following:

- Uploading Malware
- Running Programs
- Dumping Hashes
- Timestomping
- Disabling Services
- Killing Processes
- Stealing Data
- Abuse

These tasks will be performed in other Ethical hacking Labs.

3.2 Conclusion

Armitage is a front end for Metasploit that allows users to scan and exploit remote machines. If an attacker gets on the internal network, they will likely encounter more open ports and possibly unpatched systems that are protected from being directly attacked from machines on the Internet, unless that attacker penetrates the internal network. For this reason, all systems should be patched regardless of network location.

3.3 Discussion Questions

1. What would an attacker likely go after first, a server or a workstation?
2. Why might a workstation be a softer target for an attacker?
3. What is the command to enumerate a list of the available domains?
4. What is the command to view the computers in the workgroup WORKGROUP?

References

1. Microsoft Security Bulletin MS09-050 - Critical Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517): http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

2. CERT Advisory CVE-2009-3103: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-3103

3. BackTrack Linux: http://www.backtrack-linux.org/

4. Armitage: http://www.fastandeasyhacking.com/

5. Metasploit: http://metasploit.com/

