ETHICAL HACKING LAB SERIES

Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

Certified Ethical Hacking Domains: Introduction to Ethical Hacking, Scanning Networks, Enumeration, Sniffers

Document Version: 2015-08-14

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Development was 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.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.
Contents
Introduction .................................................................................................................................................. 3
Domains: Introduction to Ethical Hacking, Scanning Networks, Enumeration, Sniffers ... 3
Pod Topology ............................................................................................................................................. 4
Lab Settings .............................................................................................................................................. 5
1 Discovering Hosts ................................................................................................................................... 6
  1.1 Passive and Active Host Enumeration ................................................................................................. 6
  1.2 Conclusion .......................................................................................................................................... 13
2 Discovering Hosts with Windows Command Line Tools ......................................................................... 14
  2.1 Capture Network Traffic and then Analyze the Amount of Traffic Sent .............................................. 14
  2.2 Conclusion .......................................................................................................................................... 20
3 Discovering Hosts with Metasploit and Cain .......................................................................................... 21
  3.1 Using Metasploit to Enumerate Hosts on the Network ........................................................................ 21
  3.2 Conclusion .......................................................................................................................................... 30
References .................................................................................................................................................. 31
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

Introduction

In this lab, students will enumerate hosts on the network using various tools.

This lab includes the following tasks:

1. Discovering Hosts with Nmap and Zenmap
2. Discovering Hosts with Windows Command Line Tools
3. Discovering Hosts with Metasploit and Cain

Domains: Introduction to Ethical Hacking, Scanning Networks, Enumeration, Sniffers

Hackers will use various tools to find hosts on the network. After hosts are discovered and detailed information is gathered, the next step usually involves attacking systems.

Nmap – Nmap is a 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 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 frontend for Nmap.

Metasploit – Metasploit is an exploitation framework. Version 3 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 application software 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.

tcpdump – A Linux/UNIX program that captures network traffic. The tcpdump program comes installed on many Linux distributions by default.

Sniffer – A sniffer is used to capture network traffic. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.

Cain – A password cracking suite that will allow an attacker to crack passwords through a dictionary attack, the use of brute force, or a rainbow table. Cain, which is available from the website www.oxid.it, will not run on most computers that have anti-virus software installed, without being explicitly allowed within the anti-virus program Cain does not run on Linux or Mac OS X systems.
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.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>IP Address</th>
<th>Account</th>
<th>Password (if needed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall (Windows 2003 Server)</td>
<td>192.168.1.1</td>
<td>Administrator</td>
<td>ethical</td>
</tr>
<tr>
<td>Windows 2003 Exchange SQL</td>
<td>192.168.1.100</td>
<td>Administrator</td>
<td>P@ssw0rd</td>
</tr>
<tr>
<td>Windows 2008 Server</td>
<td>192.168.1.200</td>
<td>Admin</td>
<td>NO PASSWORD</td>
</tr>
<tr>
<td>Internal Backtrack 5</td>
<td>192.168.1.50</td>
<td>root</td>
<td>toor</td>
</tr>
<tr>
<td>Windows XP Pro</td>
<td>192.168.1.175</td>
<td>hacker</td>
<td>toor</td>
</tr>
<tr>
<td>Linux Sniffer</td>
<td>NO IP ADDRESS</td>
<td>root</td>
<td>toor</td>
</tr>
</tbody>
</table>
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

1 Discovering Hosts

Nmap, or network mapper, is free and runs on multiple platforms including Microsoft Windows, Mac, and Linux. It can be used to determine which hosts are up on the network and can then determine which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports a remote system has running.

Zenmap is a GUI frontend for Nmap, which provides the user with detailed information about the machines they are scanning. Zenmap provides details including banner messages, which are greetings made to machines connecting to a port. Using the information gathered during the scan, Zenmap will provide you with a determination of what the remote machine’s operating system is. Once an attacker determines the version of the operating system and corresponding service pack level, they can search for an exploit.

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

1.1 Passive and Active Host Enumeration

1. Open the Internal BackTrack 5 Linux system Login with the username root and password toor.
2. Type the startx command to initialize the Graphical User Environment (GUI).
   root@bt:~# startx
3. Open a terminal window by clicking on the picture to the right of the word System in the taskbar in the top of the screen in BackTrack version 5 R3.

![Figure 2: The Terminal Windows within BackTrack](image)

Before scanning the network with tools that will be detected by network sensors, we can passively listen for broadcast packets that are sent to all machines on the network.
4. Type the following to view the various switches for the tcpdump utility:

   root@bt:~# tcpdump -help

   ![tcpdump command](image)

   Figure 3: The tcpdump command

On the internal 192.168.1.0/24 network, broadcasts are sent to the broadcast address 192.168.1.255.

![Broadcast Address](image)

   Figure 4: The Broadcast Address is 192.168.1.255.

5. Type the following command to passively sniff traffic on interface eth0:

   root@bt:~# tcpdump

   ![Passive Sniffing](image)

   Figure 5: Passive Sniffing
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

Most of the IP addresses announce themselves on the network without doing any type of scan. User Datagram Protocol (UDP) NetBIOS Datagrams are sent to the network broadcast address of 192.168.1.255. Address Resolution Protocol (ARP) uses the broadcast MAC address of FF:FF:FF:FF:FF:FF. These broadcasts are sent to all machines within a single broadcast domain; meaning ARP broadcasts are not forwarded off a LAN segment.

6. **Close** the terminal window.

We will start the sniffer to examine what traffic is generated, using Nmap and Zenmap scans.

7. Log into the Linux Sniffer machine in the topology diagram with the username of **root** with the password of **toor**.

For security purposes, the password will not be displayed.

8. Type the following command to initialize the Graphical User Environment:

```
root@bt:~# startx
```

![Figure 6: Logging on to the Sniffer](image)

9. Open a terminal window by clicking on the picture to the right of Firefox in the taskbar in the bottom of the screen in BackTrack.

![Figure 7: The Terminal Window Icon within BackTrack](image)

10. After opening the terminal, you may want adjust the size of the font. To increase the font size within the terminal, click **Settings** from the terminal menu bar, select **Font**, then select **Enlarge Font**.
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

One of the nice features about some versions of BackTrack is they are not automatically assigned IP addresses through the use of DHCP, or Dynamic Host Configuration Protocol. The idea is to come on the network quietly, without being detected.

8. Only the loopback address, 127.0.0.1, is displayed when you type:

   root@bt:~# ifconfig

   Figure 9: No IP addresses, other than the Loopback Address of 127.0.0.1, are Displayed

9. Type the following command to view all available interfaces on the system:

   root@bt:~# ifconfig -a

   Figure 10: All Available Interfaces on the System
In this lab, we will capture internal traffic from Nmap and Zenmap scans with Wireshark.

10. To activate the first interface, type the following command:
    ```
    root@bt:~# ifconfig eth0 up
    ```
    ![Figure 11: Activating the First Interface](image)

11. To verify the first interface, type the following command:
    ```
    root@bt:~# ifconfig eth0
    ```
    ![Figure 12: The First Interface is activated without an IP address](image)

12. On the sniffer machine, type the following command to launch Wireshark:
    ```
    root@bt:~# wireshark
    ```
    ![Figure 13: Typing Wireshark](image)

13. Check the Don’t show the message again box and click the OK button.
    ![Figure 14: Wireshark Message](image)

Before sniffing network traffic, we want to designate the internal interface. Designating the internal interface tells Wireshark which network interface we want to see traffic from.

14. Select Capture from the Wireshark menu bar, and choose Interfaces.
15. Locate eth0 on the left side. Click the Start button on the right across from it. The scan begins; leave the scan running.

16. Open the BackTrack 5 machine on the internal network in the lab topology. In a terminal window, type the following command to conduct a ping scan to find hosts on the 192.168.1.0/24 network: root@bt:~# nmap –sP 192.168.1.*

Linux is case sensitive; use lowercase "s" and capital "P".

The results of the ping scan indicate five hosts on the 192.168.1.0/24 network.
17. For the next task, return to the Linux Sniffer machine from the lab topology. In the Wireshark window, type `arp` in the filter pane and click Apply. This filters displayed packets from the scan to only show packets using the Address Resolution Protocol (ARP). Your screen should resemble figure 16 below; notice the ARP packets. **Note: Wireshark is continuing to capture frames- Do not stop this process.**

![Wireshark Filtered ARP Packets](image)

**Figure 18: The ARP Packets**

Remember, all local area network (LAN) traffic uses MAC addresses to communicate. Address Resolution Protocol (ARP) is responsible for determining the MAC address of a machine by broadcasting an inquiry containing the machine’s IP address. Before we can ping a machine on the LAN using its IP address, ARP must first determine the MAC address so that a layer 2 frame can be constructed. A ping scan using Nmap, therefore, will display a large number of ARP requests and replies as Nmap attempts to locate and ping each machine on the network.

18. For our next task, we will use Zenmap, the GUI frontend to Nmap. Open the BackTrack 5 machine on the Internal Network in the lab topology. To start Zenmap, type `zenmap` in the terminal window.

```
root@bt:~# zenmap
```

![Typing zenmap](image)

**Figure 19: Typing zenmap**
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

19. In the target box, type the network ID of 192.168.1.0/24, and click **Scan**.

![Figure 20: The Zenmap Target](image)

After some time elapses, Zenmap will display the IP addresses and OS type detected. Please be patient, as this process may take several minutes (approx. 5 minutes). Upon completion, the list of discovered hosts and their detected operating systems will be automatically displayed on the left within the Zenmap window.

![Figure 21: The List of Discovered IP addresses](image)

20. Return to the **Linux Sniffer** machine from the lab topology. Type **tcp.flags.reset==1** in the Wireshark filter pane and click **Apply**.

![Figure 22: TCP Reset Packets](image)

1.2 **Conclusion**

There are two options for detecting other hosts on the network:

- Passively listening for devices to "announce" their presence on the wire.
- Actively scanning for hosts using a tool like **Nmap** or **Zenmap**.
2 Discovering Hosts with Windows Command Line Tools

While tools like Nmap, Zenmap, tcpdump, and Wireshark will allow you to enumerate hosts; you can also enumerate hosts with some of the built-in Windows commands. In this exercise, we will use Wireshark to capture the network traffic, and then analyze the amount of traffic sent to the broadcast address by the Windows machines.

2.1 Capture Network Traffic and then Analyze the Amount of Traffic Sent

1. On the Linux Sniffer machine, stop the Wireshark capture by clicking the stop icon (below go).

![Figure 23: Stopping Wireshark](image1)

2. Select Capture from the Wireshark Menu bar, and choose Interfaces.

![Figure 24: Capture Sub-Menu](image2)

3. Locate eth0 on the left side. Click the Start button on the right across from it.

![Figure 25: Starting the Capture](image3)

4. Click Continue without Saving when you receive the warning message.

![Figure 26: Continue Without Saving](image4)
5. In the Wireshark filter pane, type `ip.addr == 192.168.1.255` and click **Apply**:

![Wireshark Filter](image)

**Figure 27: IP address Filter**

After a short while, you will see Windows broadcast packets appear in the network traffic.

![Broadcast Traffic](image)

**Figure 28: Broadcast Traffic**

6. Log into the **Windows XP Pro** system using the **hacker** account with the password of **toor**.

![Logging in as hacker](image)

**Figure 29: Logging in as hacker**

7. Open the command prompt on the Windows XP machine by double-clicking the desktop shortcut.

![Command Prompt](image)

**Figure 30: A Shortcut to the Command Prompt**
8. Type the following to enumerate the other computers in your workgroup:
   \C: > net view

   **Figure 31: The net view command**

9. Type the following command to enumerate the domain list:
   \C: > net view /domain

   **Figure 32: Net View with Options**

10. Type the following command to view the computer’s in XYZCompany’s domain:
   \C: > net view /domain:XYZcompany

   **Figure 33: Viewing computers in a Different Workgroup**
11. Type the following to view the computers in the domain WORKGROUP.

C:\>net view /domain:WORKGROUP

```
C:\>net view /domain:WORKGROUP
Server Name                Remark
\\WINFILE
\\WINXP
The command completed successfully.
```

Figure 34: Viewing Workgroup Computers

Return to the Linux Sniffer machine. You can look at all of the browser traffic to see all of the computer and domain names.

12. To view computers and domains, type browser in the filter pane and click Apply:

You may have less output than what is displayed below. Wireshark is continuing to capture packets, so the list may continue to grow.

```
<table>
<thead>
<tr>
<th>Filter</th>
<th>browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Time</td>
</tr>
<tr>
<td>26</td>
<td>150.230242</td>
</tr>
<tr>
<td>26</td>
<td>150.230242</td>
</tr>
<tr>
<td>26</td>
<td>150.230242</td>
</tr>
<tr>
<td>25</td>
<td>149.310777</td>
</tr>
<tr>
<td>25</td>
<td>149.310777</td>
</tr>
<tr>
<td>25</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
<tr>
<td>24</td>
<td>149.310777</td>
</tr>
</tbody>
</table>

Figure 35: Browser Packets

We have determined the following information by using the net view command:

<table>
<thead>
<tr>
<th>Work Group Name</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORKGROUP</td>
<td>WINFILE, XP, FW</td>
</tr>
<tr>
<td>XYZCOMPANY</td>
<td>SERVER</td>
</tr>
</tbody>
</table>

Now that we have names, we can also determine the IP address of each machine.
13. Return to the **Windows XP Pro** machine. Type the following command to identify the IP address of the **fw** machine:

```
C:\> ping fw
```

![Figure 36: Pinging FW](image)

The IP address for the machine named fw is identified as 192.168.1.1.

14. Type the following command to identify the IP address of the **winfile** machine:

```
C:\> ping winfile
```

![Figure 37: Pinging WINFILE](image)

The IP address for the machine named winfile is identified as 192.168.1.200.
15. Type the following command to identify the IP address of the **server** machine:

   C:\> ping server

   C:\> ping server [192.168.1.100] with 32 bytes of data:

   Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

   Ping statistics for 192.168.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milliseconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms

   **Figure 38: Pinging Server**

   The IP address for the machine named server is identified as 192.168.1.100.
   We will not need to identify the IP address for our own machine named XP.

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>SERVER</td>
<td>192.168.1.100</td>
</tr>
<tr>
<td>XP</td>
<td>192.168.1.175</td>
</tr>
<tr>
<td>WINFILE</td>
<td>192.168.1.200</td>
</tr>
</tbody>
</table>

16. **Return to the Linux Sniffer machine**. You can view the Address Resolution Protocol (ARP) traffic involved in the IP address discovery by typing `arp` in the Wireshark filter pane and clicking **Apply**.

   **Figure 39: ARP Packets**
17. On the Linux Sniffer machine, stop the Wireshark capture by clicking the stop icon (below Go).

![Stopping Wireshark](image)

**Figure 40: Stopping Wireshark**

18. **Close** all windows on the *Internal* BackTrack 5 machine.

Here is a list of the commands that were used during this task to enumerate Windows hosts.

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>net view</td>
<td>Enumerates the machines within the same workgroup</td>
</tr>
<tr>
<td>net view /domain</td>
<td>Enumerates all workgroups and domains</td>
</tr>
<tr>
<td>net view /domain:workgroup</td>
<td>Enumerates the machines in the workgroup WORKGROUP</td>
</tr>
<tr>
<td>net view /domain:XYZcompany</td>
<td>Enumerates the machines in the domain XYZcompany</td>
</tr>
</tbody>
</table>

### 2.2 Conclusion

While there are scanning tools available like Nmap and Zenmap that will scan a network, there are also built-in tools that will allow a user to enumerate hosts on a network, even if they do not have administrative rights. There are situations where hackers need to find out information about other hosts on the network, but cannot install programs. Using built-in commands like net view will allow for the enumeration of hosts.
3 Discovering Hosts with Metasploit and Cain

You can enumerate hosts with third party tools like Nmap, Zenmap, tcpdump, and Wireshark or by using built-in Windows commands. There are also sophisticated attack tools, like Metasploit and Cain, which will allow you to view hosts on the network.

3.1 Using Metasploit to Enumerate Hosts on the Network

1. On the Internal BackTrack 5 machine, type the following to launch Metasploit:
   
   root@bt:~# msfconsole

   ![Figure 41: Launching Metasploit]

   A random Metasploit banner message will appear and the current version number will be displayed.

   ![Figure 42: Metasploit Banner]

   You can type the **banner** command at **msf >** to display a different banner.
We will now search for the scanner modules that exist within Metasploit.

2. To search for all of the available scanners within Metasploit, type the following:
   
   ```
   msf > search scanner
   ```

   ![Figure 43: Searching for Scanners](image)

   There are a large number of scanners within Metasploit, including IPv6 scanners.

   ![Figure 44: A Partial List of Metasploit Scanners](image)

3. To select the Metasploit scanner that will perform an arp sweep, type:

   ```
   msf > use auxiliary/scanner/discovery/arp_sweep
   ```

   ![Figure 45: Using the arp Sweep Scanner](image)
4. Type the following command to see the available options for the arp scanner:
   `msf auxiliary(arp_sweep) > show options`

   ![Figure 46: The Options for the Scanner](image)

5. Type the following command to set 192.168.1.0/24 as the target network:
   `msf auxiliary(arp_sweep) > set RHOSTS 192.168.1.0/24`

   ![Figure 47: Setting the Target Network](image)

6. Type the following command to verify that the network range is correct:
   `msf auxiliary(arp_sweep) > show options`

   ![Figure 48: Verifying the Network Range](image)

Before running the scan, we will start capturing on the **Linux Sniffer** machine again.

7. Select **Capture** from the Wireshark menu bar, and choose **Interfaces**.

   ![Figure 49: Capture Sub-Menu](image)
8. Locate eth0 on the left side. Click the Start button on the right across from it.

![Wireshark: Capture Interfaces](image)

Figure 50: Starting the Capture

9. Click Continue without Saving when you receive the warning message.

![Save capture file before starting a new capture?](image)

Figure 51: Continuing without Saving

10. Return to the Internal BackTrack 5 machine. Type the following command to initiate the arp sweep process:

```
msf auxiliary(arp_sweep) > run
```

![msf auxiliary(arp_sweep) > run](image)

Figure 52: ARP Sweep is completed

On the Linux Sniffer machine, you will notice a large number of ARP packets in Wireshark.

![ARP Packets Generated from ARP Sweep](image)

Figure 53: ARP Packets Generated from ARP Sweep
11. To go back one level to the msf prompt and exit the arp_sweep scanner, type the following command:
   `msf auxiliary(arp_sweep) > back`

   ![Figure 54: Moving Back One Level](image)

12. To use the NetBIOS name scanner, type the following command:
   `msf > use auxiliary/scanner/netbios/nbname`

   ![Figure 55: The NetBIOS Scanner](image)

13. Type the following command to display the module options:
   `msf auxiliary(nbname) > show options`

   ![Figure 56: Showing Options](image)

14. Type the following command to set 192.168.1.0/24 as the target network:
   `msf auxiliary(nbname) > set RHOSTS 192.168.1.0/24`

   ![Figure 57: Setting the Network](image)

15. Type the following command to enumerate the netbios names of the computers:
   `msf auxiliary(nbname) > run`

   ![Figure 58: The List of Computer Names](image)
16. On the Linux Sniffer machine, type `nbns` in the Wireshark filter pane and click Apply.

![Wireshark Filter Result](image)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>27.286746</td>
<td>192.168.1.175</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB Rk&lt;20&gt;</td>
</tr>
<tr>
<td>259</td>
<td>27.28919</td>
<td>192.168.1.1</td>
<td>192.168.1.175</td>
<td>NBNS</td>
<td>Name query response NB 216.1.1.1</td>
</tr>
<tr>
<td>305</td>
<td>92.692696</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>306</td>
<td>93.442183</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>307</td>
<td>94.193112</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>328</td>
<td>334.317242</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>329</td>
<td>335.000670</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>390</td>
<td>335.816630</td>
<td>192.168.1.1</td>
<td>192.168.1.255</td>
<td>NBNS</td>
<td>Name query NB WORKGROUP&lt;1b&gt;</td>
</tr>
<tr>
<td>375</td>
<td>610.395192</td>
<td>192.168.1.50</td>
<td>192.168.1.0</td>
<td>NBNS</td>
<td>Name query NBSTAT *&lt;00&gt;&lt;00&gt;&lt;00&gt;&lt;0</td>
</tr>
<tr>
<td>380</td>
<td>610.497156</td>
<td>192.168.1.50</td>
<td>192.168.1.1</td>
<td>NBNS</td>
<td>Name query NBSTAT *&lt;00&gt;&lt;00&gt;&lt;00&gt;&lt;0</td>
</tr>
<tr>
<td>381</td>
<td>610.497277</td>
<td>192.168.1.1</td>
<td>192.168.1.50</td>
<td>NBNS</td>
<td>Name query response NBSTAT</td>
</tr>
<tr>
<td>479</td>
<td>610.831713</td>
<td>192.168.1.50</td>
<td>192.168.1.100</td>
<td>NBNS</td>
<td>Name query NBSTAT *&lt;00&gt;&lt;00&gt;&lt;00&gt;&lt;0</td>
</tr>
<tr>
<td>480</td>
<td>610.831818</td>
<td>192.168.1.100</td>
<td>192.168.1.50</td>
<td>NBNS</td>
<td>Name query response NBSTAT</td>
</tr>
</tbody>
</table>

**Figure 59: NetBIOS Name Service Packets**

Next, we will enumerate hosts on Windows XP, using the attack tool Cain.

17. On the Windows XP Pro machine, double-click the shortcut to Cain on the desktop.

![Cain Shortcut](image)

**Figure 60: The shortcut to Cain**

18. Click OK to the warning from Cain that the Windows Firewall is enabled.

![Cain Warning](image)

**Figure 61: Cain Warning**
19. To use the scanning and enumeration features of Cain, Click on the Sniffer tab.

![Cain sniffer Tab](image)

**Figure 62: Cain sniffer Tab**

20. Click the **Start/Stop Sniffer** icon, which is a picture of a Network Interface Card (NIC).

![Starting the Sniffer](image)

**Figure 63: Starting the Sniffer**

21. Click **OK** when the configuration dialogue box appears.

![Configuration Dialog Box](image)

**Figure 64: Configuration Dialog Box**
22. After clicking **OK** to the Configuration Dialog, click the **Start/Stop Sniffer** icon.

![Starting the Sniffer](image)

**Figure 65: Starting the Sniffer**

23. Right-click in the white space and select **Scan MAC Addresses**.

![Scan MAC Addresses](image)

**Figure 66: Scan MAC Addresses**

24. Scan all hosts in the Subnet by clicking **OK** in the MAC Address Scanner dialog window.

![MAC Address Scanner Dialog Window](image)

**Figure 67: MAC Address Scanner Dialog Window**
IP addresses and corresponding MAC addresses will be displayed in the sniffer pane.

Figure 68: Results of the Scan

25. Right-click on 192.168.1.1 and select **Resolve Host Name**.

The Host Name of FW will be displayed in the hostname column.

Figure 70: Host Name of FW

26. Right-click on 192.168.1.100 and select **Resolve Host Name**.

The Host Name of server.xyzcompany.com will be displayed in the hostname column.

Figure 72: Host Name of server.xyzcompany.com
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

27. Right-click on 192.168.1.200 and select **Resolve Host Name**.

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>OUI fingerprint</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>00C2931571E</td>
<td>VMware, Inc.</td>
<td>FW</td>
</tr>
<tr>
<td>192.168.1.50</td>
<td>00C294B5CBE</td>
<td>VMware, Inc.</td>
<td></td>
</tr>
<tr>
<td>192.168.1.100</td>
<td>00C2943C90D</td>
<td>VMware, Inc.</td>
<td>server.xyzcompany.com</td>
</tr>
<tr>
<td>192.168.1.200</td>
<td>00C29C4994B</td>
<td>VMware, Inc.</td>
<td>WINFILE</td>
</tr>
</tbody>
</table>

**Figure 73: Resolving the Host Name**

The Host Name of WINFILE will be displayed in the hostname column.

**Figure 74: Host Name of WINFILE**

3.2 **Conclusion**

Tools such as Cain and Metasploit can be used to enumerate hosts on a network. They can provide information about IP addresses and hostnames of machines on the network. ARP or broadcast packets are generated when hosts are enumerated.
Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

References

1. Wireshark: www.wireshark.org
2. tcpdump: http://www.tcpdump.org/
5. Metasploit: www.metasploit.com