Lab 7: Introduction to Pen Testing (NMAP)

Aim:

To provide a foundation in understanding of email with a focus on NMAP.

Time to complete: Up to 60 minutes.

Activities:

- **Complete Lab 7**: NMAP.
- **Complete Test 7**.

Leaning Activities:

At the end of these activities, you should understand:

- How to determine key details related to basic pen testing.
- The presence of each of the scan and how they can be observed in a trace.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- How might you use NMAP to determine the vulnerabilities on hosts and servers?
- Why would you want to detect NMAP activity on your network?
- Why would NMAP uses an ARP scan rather than an ICMP scan?
- Knowing that SYN floods might be blocked from the firewall, why might an intruder use a FIN scan?

Lab 7: Intro to Pen Testing (NMAP)

1 Details

Aim: To provide a foundation in understanding NMAP.

In this lab (Figure 1), we will use a local Windows hosts to scan the Windows 2003 and Ubuntu virtual machines. The addresses we will use are:

- [Host IP] which is the IP address of your Windows host.
- [Windows2003 IP] which is the IP address of the Windows 2003 virtual image.
- [Ubuntu IP] which is the IP address of the Ubuntu virtual image.

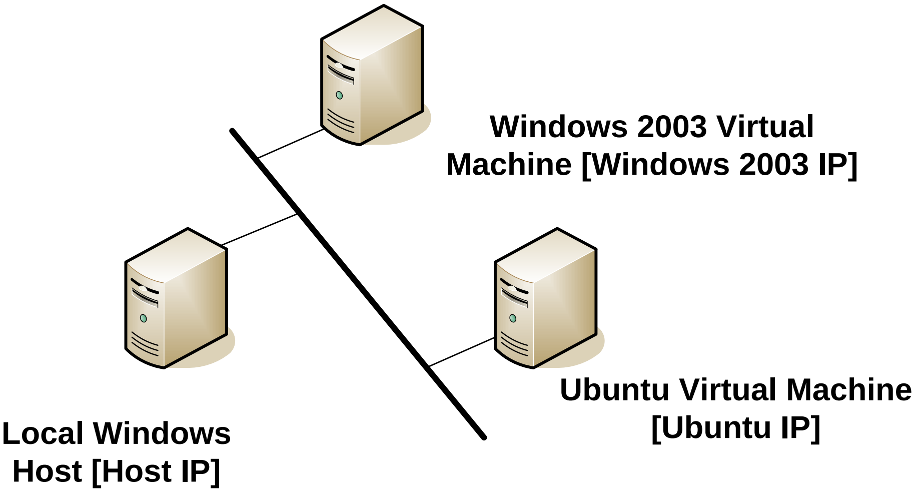
Windows 2003 Virtual Machine [Windows 2003 IP]
Local Windows Host [Host IP]
Ubuntu Virtual Machine [Ubuntu IP]

Figure 1: Network setup

2 Discovering the Network

L1.1 On your Windows host, download and install NMAP:

http://nmap.org/dist/nmap-6.40-setup.exe

L1.2 Start the Ubuntu and Windows 2003 instances, and determine the IP addresses:

Using IPCONFIG, determine your Windows host IP address and subnet mask (for the virtual network connection) [Host IP]:

Using IPCONFIG, determine your Ubuntu host IP address and subnet mask [Ubuntu IP]:

Using IPCONFIG, determine your Windows 2003 host IP address and subnet mask [Windows 2003 IP]:

3 Discovering and Testing Services

L1.3 Determine the services which are running on each of your devices using:

On your Windows host, run the command netstat –a**, and outline some of the the services which are running on your host (define the port number and the name of the service and only pick off the LISTENING status on the port):**

For the Ubuntu Virtual Machine, and run the command netstat –l**, and outline some of the services which are running on your host (define the port number and the name of the service):**

For the Windows 2003 Virtual Machine, and run the command netstat –a**, and outline some of the services which are running on your host (define the port number and the name of the service and only pick off the LISTENING status on the port):**

L1.4 Next we will determine if these services are working. There should be a Web server working on each of the virtual machines (Ubuntu and Windows 2003), so from the Windows host and using a Web browser, access the home page on each:

http://[Ubuntu IP]

http://[Windows2003 IP]

Can you access each of these Web site?

L1.5 Next we will determine if these services are working using a command line. As we have seen there should be a Web server working on each of the virtual machines (Ubuntu, and Windows 2003). From your Windows host, undertake the following:

telnet [Ubuntu IP] 80
then enter:
GET /

telnet [Windows 2003 IP] 80
then enter
GET /

What is returned for each of the accesses:

L1.6 There should be an FTP server working on Ubuntu and Windows 2003. Access these by performing the following:

```
telnet [Ubuntu IP] 21
then enter:
USER napier
PASS napier123
QUIT

telnet [Windows 2003 IP] 21
then enter
USER Administrator
PASS napier
QUIT
```

Outline the messages that you received:

What happens to each of these when you try with an incorrect username and password:

L1.7 On both Ubuntu and Windows 2003 instances you will see that the **TELNET** service is running, which allows for remote access. Using the command:

```
telnet [Ubuntu IP]
telnet [Windows 2003 IP]
```

Did you manage to logon to these services:

What were the user names and passwords you have used:

L1.8 On the Ubuntu instance you will see that the **VNC** service is running, which is the remote access service. Download a VNC client from:

http://www.realvnc.com/download/get/1293/

From your Windows host, access the VNC service, and see what happens:

What does this service do:

What happens when you try to access the Windows 2003 remote access service from the Remote Desktop on your Windows host (to access this run Remote Desktop Connection from the Start->Run command box):

L1.4 Next we will assess the SMTP service running on the Windows 2003 virtual machine. From your Windows machine console run a service to access SMTP:

```
telnet [Ubuntu IP] 25
```

Next enter the commands in bold:

```
220 napier Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959 ready
    at  Sun, 2 Dec 2009 21:56:01 +0000
help
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN
    BDAT VRFY
helo me
250 napier Hello [192.168.75.1]
mail from: email@domain.com
250 2.1.0 email@domain.com....Sender OK
rcpt to: fred@mydomain.com
250 2.1.5 fred@mydomain.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
From: Bob <bob@test.org>
To: Alice <alice@test.org >
Date: Sun, 20 Dec 2013
Subject: Test message

Hello Alice.
This is an email to say hello
.
250  2.6.0  <NAPIERMp7lzvxrMVHFb00000001@napier>  Queued  mail  for
    delivery
```

L1.5 On the Windows 2003 virtual machine, go into the `C:\inetpub\mailroot\queue` folder, and view the queued email message.

Was the mail successfully queued? If not, which mail folder has the file in?

Outline the format of the EML file?

4 Scanning with NMAP

L1.9 Determine the IP address of your hosts (from L1.2), and find the common part. Then replace the last digit with a zero. For example, if your network addresses are 192.168.47.21 and 192.168.47.10, then the network address is 192.168.47.0/24.

What is this network address:

L1.10 Port sweep of Web Servers on the network. On your Windows host, **run Wireshark** and capture traffic from your virtual network interface. We will now discover the network, so open up a console on your Windows host, and then run NMAP with the command:

```
nmap –p 80 [Network Address of Your Network]/24
```

What is the results from NMAP:

What can you observe from your Wireshark trace:

Why do we see an ARP scan, and how does it determine that the Web port is open:

L1.11 Port sweep the servers. On your Windows host, **run Wireshark** and capture traffic from your virtual network interface. Now from your Windows host, scan each of your machines with:

```
nmap  [Ubuntu IP]
```

What is the results from NMAP:

What can you observe from your Wireshark trace:

Does the scan tie-up with the scan you did previously in L1.3:

```
nmap  [Windows2003 IP]
```

What is the results from NMAP:

What can you observe from your Wireshark trace:

Does the scan tie-up with the scan you did previously in L1.3:

L1.12 **Now we will perform different scans on our hosts.** For each, **run Wireshark** and run NMAP against the hosts and observe the results:

Perform a SYN scan

nmap –sS [Ubuntu IP]
nmap –sS [Windows2003 IP]

What can you observe from the Wireshark trace:

Perform a Connect scan

nmap –sT [Ubuntu IP]
nmap –sT [Windows2003 IP]

What can you observe from the Wireshark trace:

What is the difference between the two scans:

Perform a NULL scan

nmap –sN [Ubuntu IP]
nmap –sN [Windows2003 IP]

What can you observe from the Wireshark trace:

Which Wireshark filter will display only the scan:

Perform a FIN scan

nmap –sN [Ubuntu IP]
nmap –sN [Windows2003 IP]

What can you observe from the Wireshark trace:

Which Wireshark filter will display only the scan:

Perform a XMAS Tree scan:

nmap –sN [Ubuntu IP]
nmap –sN [Windows2003 IP]

Which flags are set for a XMAS tree scan:

Which Wireshark filter will display only the scan:

L1.13 Operating System scan. On your Windows host, **run Wireshark** and capture traffic from your virtual network interface. Now from your Windows host, scan each of your machines with:

nmap -O [Ubuntu IP]
nmap -O [Windows 2003 IP]

What are the results from the scan:

Did it manage to determine the correct operating system.

L1.14 Scan you neighbours host. Determine your neighbours IP address, and now determine:

The operating system they are running:

Some of the services they are running:

Perform a XMAS scan on the host, and determine the TCP ports which are open:

L1.15 Be careful. Now can the local IP address range on your local network. Be sure you get the IP network address correct! Only use a /24 mask from your home network.

Outline some of the hosts who are on-line