Nmap and Reconnaissance – Lab 1
CSCD 434

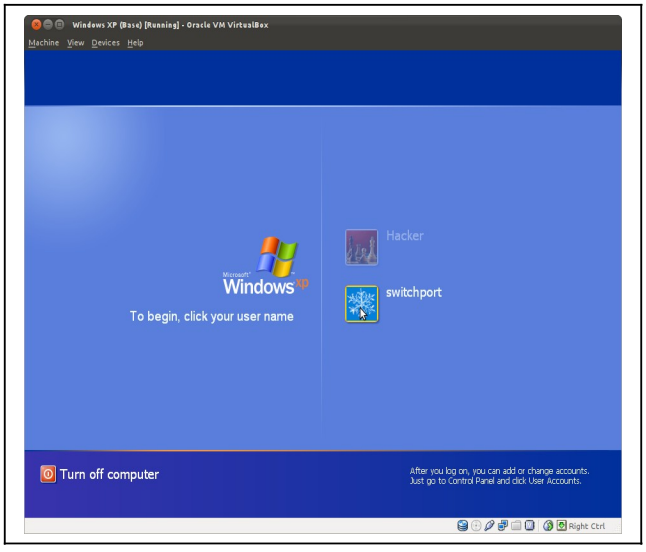
Nmap is arguably the most widely used network scanner around. This lab will give you a introduction into using Nmap to do some simple scans and get you using many of the more obscure features within Nmap.

Scanning in general is extremely important when conducting scans anything from general networking and systems tasks to penetration testing and vulnerability assessment. There is one key difference between the two types of scanning however. While conducting a penetration test you want to be as quiet as possible whereas during general system and network administration you are not really concerned with being quiet because you own the network or at least have permission to use the network.

First on your lab machine start the Vulnerable Windows XP machine which we will practice scanning. I believe the machines start right up, but if not, go ahead and log into the machine as the user 'Switchport'.

If you are doing these at home you can download a copy of Windows XP SP2 from MSDNAA and configure it using the following guide:

Post Install: http://www.offensive-security.com/metasploit-unleashed/Windows_XP_Post_Install
Setting Up additional Services: http://www.offensive-security.com/metasploit-unleashed/Setting_Up_Additional_Services
Creating a Vulnerable Web App: http://www.offensive-security.com/metasploit-unleashed/Creating_A_Vulnerable_Webapp



1) First thing we want to do is verify that we have an routable IP address on the Windows XP workstation. Do this by changing the VirtualBox networking card to 'bridged' if it is not

already. By default they should all be bridged in the lab. You can open up a window and type: ipconfig to see the ip number of the windows machine. Write that ip number down.

2) Open up a terminal on your host machine and ping the windows host to verify connectivity.

> ping <your windows xp ip>

3) Once you can communicate to your Windows box, do a basic default nmap scan to see what happens. By default nmap will ping your target machine first to verify that it can actually scan it. This is important because often times ping or ICMP is disallowed on networks or between networks. In this case you will have to adjust your scan to be able to see those machines.

> nmap <your windows xp ip>

Note: you can also scan ranges of IPs or lists (text files). See some examples below:

> nmap 192.168.30.0/24
> nmap 192.168.30.1 - 100
> nmap 192.168.30.100
> nmap -iL <file list of hosts>

4) Once you verify that there are some services listening. Lets see what other options we might want to use against this target. To see all of Nmap scan filters just type, Nmap to see a list of the command line arguments that can be supplied.

> nmap

5) There are many options for just about every situation. What if we want to figure out what version of services are listening on a remote host? For this we will use the -sV flag.

> nmap -sV <you windows xp ip>

There are many other types of scans. We will not cover each of them but look at least at those three and get comfortable using them. Try to understand under what circumstances you would actually use them.

-PN is used if the remote host/network does not allow ICMP. this will treat all the hosts as up and continue with the scan.

-T5 will make nmap scan faster 0-5 with 5 being the fastest

-sS is the “silent” scan. This is a SYN scan and generally will not trigger many firewalls as there is never a complete connection made.

6) Nmap supports more than just basic scanning and service enumeration. It is also fully scriptable. There are many pre-built scripts that come with Nmap that do various tasks. One such task is to scan Netbios ports to see if they are vulnerable to any known exploits.

To see a list of nmap pre-built scripts type the following command:

> ls /usr/share/nmap/scripts

7) Lets look for the Netbios script (smb-check-vulns.nse)

> ls /usr/share/nmap/scripts | grep smb

8) Our windows XP machine is vulnerable to several different attack vectors but for this example we will focus on the netbios vulnerabilities. Lets scan our Windows XP machine with this script and see what vulnerabilities it finds.

> nmap --script smb-check-vulns.nse -p 445 <your windows xp ip>

Write down what this scan reports.
You will notice that we added an additional command here. the -p flag allows the narrowing down of the default ports to either a single port or range of ports. For example, if you know are scanning a bunch of web servers and are only interested in the two standard HTTP(s) ports you would use the following command:

> nmap -p 80,443 <range of web hosts>

Or you might want to only scan the first 110 ports of a host

> nmap --script smb-check-vulns.nse -p445 <your windows xp ip>

```
Starting Nmap 5.21 ( http://nmap.org ) at 2012-04-09 14:45 PDT
NSE: Script Scanning completed.
Nmap scan report for 192.168.30.166
Host is up (0.00039s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-check-vulns:
|   MS08-067: LIKELY VULNERABLE (host stopped responding)
|   Conficker: UNKNOWN; got error SMB: Failed to receive bytes after 5 attempts: EOF
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|_  SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
```

9) DNS enumeration is another important thing to look at while scanning. There are many commands available on Linux that help with this dig, host, nslookup, and whois to name a few.

You can also use several online resources. Lets look at google and see what types of DNS services are available. Keep in mind that some of these commands use ICMP and ICMP is blocked outside of the EWU network. This is why you cannot ping google or anything from inside the EWU network.

Lets look at the dig command and its options

> dig -h

From here lets try and find out the IP address of google web servers or A records. This is the default dig type.

> dig google.com

You should see a list of A records for google.com. Now change the type and get a list of google.com's MX records

> dig -t MX google.com

10) Another interesting command is the 'host' command. Just do a host against google.com and see what happens.
> host google.com

11) Whois is another powerful tool. It will return the names of DNS servers among other information. Type in, whois google.com . How many DNS servers are returned ? What are there names?

Questions

1) Scan the entire 192.168.30.0/24 subnet. What hosts addresses have SSH running?

2) Given the scan of your Nmap and what services are available. What other standard Nmap scripts would you use to gather more information about this host? Try running some of them and see the results. List the ones you tried that actually showed some decent output. You can look up more information on the scripts here, http://nmap.org/book/nse-usage.html

3) What netbios vulnerability was our Windows XP vulnerable to?

4) What is an A record?

5) What is an MX record?

6) Name the aol.com MX records.

7) What are the aol.com A records?

8) Use whois to find aol.com DNS records

9) What are the IP addresses that aol.com lies in?

Turn in ….
Answers can be emailed to me embedded in the email or as a separate document.
Put, CSCD434 – Lab 1 in the subject line.