Lab: Network Scanning using nmap

Goal of the Lab Exercise

After this lab, you should be able to

- Use Nmap in the command line to scan a host/network to identify possible vulnerable location in the host/network.

Requirements

1. For this Lab we will be using Kali Linux and Metasploitable 2 virtual machines or any other target machine (such as windows xp vm)
2. Metasploitable username and password is msfadmin/msfadmin
3. Review the reference slides posted on lecture page in before you begin this lab.

Introduction "Nmap - the Network MAPper"

To crack into a computer system, an attacker must target a machine and identify which ports the machine is listening before a system can be compromised. The attacker can sweep networks and locate vulnerable targets using scanners such as Nmap. Once these targets are identified with scanners such as Nmap, the attacker may scan for listening ports. Nmap also uses TCP stack fingerprinting to accurately determine the type of machine being scanned.

There are a few graphical front ends; our lab exercise will focus on using Nmap the **command-line**.

References

- nmap manual

How to use Nmap?

The usage syntax of Nmap is fairly simple. Options to 'nmap' on the command-line are different types of scans that are specified with the -s flag. A ping scan, for example, is "-sP". Options are then specified, followed by the hosts or networks to be targeted.

Nmap is very flexible in specifying targets. Simply scan one host or scan entire networks by pointing Nmap to the network address with a "/mask" appended to it. In addition, Nmap will allow you to specify networks with wild cards, such as 192.168.100.*, which is the same as 192.168.100.0/24. Or the range of target hosts can be indicated as follows: **192.168.100.103-106**

Task 1: Getting started with nmap

1) man nmap
2) What do the following switches do? ○ -sn

- -PO
- -PS
- -PU
- -sO
- -sV
- -O

Task 2: Using nmap to conduct a reconnaissance of your network

1. Use a broad ping scan to determine the hosts that are "up" on a portion of your lab network

   nmap -n -sn IPaddress

   i. Record the results.
   ii. Why is the -n option used? What happens if you rerun this command without the -n option?

2. Conduct an IP protocol ping (switch -PO / -PS / -PU) on the Common Network hosts. Note that for this scan "nmap needs to read raw responses off the wire"; you may need to use sudo to have sufficient privilege.

   i. How many TCP ports are open on each?
   ii. Are there any UDP ports open on any machine?

3. Conduct an IP protocol ping on yourself.
   i. How many ports are open?

4. Conduct an IP protocol scan (switch -sO) on target host; note that you may have to use sudo to have sufficient privilege for this scan. Be patient, this will take a while.
   i. Are the results different than that attained with the IP protocol ping? Explain.

5. *nmap* is often capable of determining the operating system of a scanned host. {Hint: read the **OS Detection** section of the man pages and again note that you may need to use sudo to have sufficient privilege.}

Which OS is running on the host? "OS Fingerprinting"

Often an intruder may be more familiar with exploits for a particular operating system, and may be looking for machines he's able to compromise easily. A common option is TCP/IP fingerprinting with the **"-O" option** to determine the remote operating system. **This has to be combined with a port scan and not a ping scan.** Nmap accomplishes this by sending different types of probes to the host, which will narrow the target operating system. Fingerprinting the TCP stack includes such techniques as FIN probing to see what kind of response the target has, BOGUS flag probing to see the remote host's reaction to undefined flags sent with a SYN packet, TCP Initial Sequence Number (ISN) sampling to find patterns of ISN numbers, as well as other methods of determining the remote operating system.

i. What operating system does *nmap* think your Server VM is running?
ii. What is its MAC address?
iii. What operating system does nmap think your Linux VM is running?

6. *nmap* is also often able to determine the version number of various services running as software applications Hint: read the **Service/Version Detection** section of the man pages.

   i. Investigate how to restrict the application scans to specific sets of port numbers, otherwise your scans may take a long time to complete.
   ii. What version of ssh (or choose any other service) is running on your target host?
   iii. What web server is running on your target host?

NOTE: depending on your target host, your answers will vary. You are more than welcome to test any of your OWN home machine as target and do the nmap scanning.

7. **Test if any (vulnerable) services available? "Port Scanning"**

- Different types of port scans are provided by Nmap: TCP connect, TCP SYN, Stealth FIN, Xmas Tree, and Null, as well as UDP scans. Demonstrate at least a few of these scans.