Lab 09: NMap Lab Exercise

1. Goal of the Lab Exercise

After the lab exercises, the students should be able to use NMAP in command line to scan a host/network, so to find out the possible vulnerable points in the hosts.

2. Introduction

In order to crack into a computer system, an attacker has to find a target machine, and then find out what ports the machine is listening on before a system can be compromised. By using scanners such as Nmap, the attacker are able to sweep networks and look for vulnerable targets. Once these targets are identified, an intruder is able to scan for listening ports. Nmap can also use TCP stack fingerprinting to accurately determine the type of machine being scanned.

Nmap can be downloaded free of charge from <http://www.insecure.org/nmap>. There are a few graphical front ends; however, our lab exercise will focus on using Nmap in the **command-line**.

3. 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's functionality is greatly increased when run as root, because nonsuper-users don't have the ability to create the custom packets that Nmap utilizes. In our exercise, the students are given the root privilege.

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 10.6.1.\*, which is the same as 10.6.1.0/24.

3.1 Which hosts are up now?   (Ping Sweeping)

Intruders are able to sweep entire networks by looking for targets with Nmap. This is usually done with a ping scan by using the "-sP" flag. By default, Nmap will send an ICMP echo and a TCP ACK to each host it scans. Hosts that respond to either will be considered by Nmap to be up. In this example, scan all hosts on the 10.0.0.0 network.

# nmap -sP 10.0.0.0/24

Sometimes you may merely want to check the availability of a system without sending ICMP echo requests, which may be blocked by some sites. In this case, a TCP "ping" sweep can be used to scan a target's network. A TCP "ping" will send an ACK to each machine on a target network. Machines that are up should respond with a TCP RST. To use the TCP "ping" option with a ping scan, include the "-PT" flag to target a specific port on the network you're probing. In our example, we'll use port 80 (http), which is the default, and it will probably be allowed through the target's border routers and possibly even its firewall. **Note that the targeted port does not need to be open on the hosts that are being probed to determine if the machine is up or not.** Launch this type of scan as follows:

# nmap -sP -PT80 10.0.0.0/24

When a potential intruder knows which machines on the target's network are alive, typically the next step is port scanning.

3.2 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.

3.2.1 TCP connect

When an attacker is using TCP connect scans, because Nmap will use the connect() system call to open connections to interesting ports on the target host and complete the 3-way TCP handshake, the probe is easily detected by the target host. Logs on the host machine will show these ports being opened by the attacker. A TCP connect scan is used with the "-sT" flag as:

# nmap -sT 10.0.0.1

3.2.2 Stealth Scanning

What if an attacker wants to scan a host without being logged on the target machine? TCP SYN scans are less prone to logging on the target's machine, because a full handshake never completes. A SYN scan starts by sending a SYN packet, which is the first packet in TCP negotiation. Any open ports will respond with a SYN|ACK, as they should. However, the attacker sends a RST instead of an ACK, which terminates the connection. The advantage is that the 3-way handshake never completes, and fewer sites will log this type of probe. Ports that are closed will respond to the initial SYN with a RST, allowing Nmap to determine that the host isn't listening on that port. **This command might require root privileges** The "-sS" flag will launch a SYN scan against a host or network as:

# nmap -sS 10.0.0.1

Although SYN scans are more likely to be unnoticed, they can still be detected by some intrusion detection countermeasures. The Stealth FIN, Xmas Tree, and Null scans are used to evade packet filters and firewalls that may be watching for SYN packets directed toward restricted ports. These three scans should return a RST for closed ports, whereas open ports should drop the packet. A FIN "-sF" scan will send a FIN packet to each port, whereas the Xmas Tree scan "-sX" turns on the FIN, URG, and PUSH flags, and a Null Scan "-sN" turns off all flags. **Because of Microsoft's incompliance with TCP standards, the FIN, Xmas Tree, and Null scans are only effective on non-Microsoft operating systems.**

3.2.3 UDP Scanning

Using the UDP scan "-sU" an attacker can determine what ports are open to UDP on a host. Nmap will send a 0-byte UDP packet to each port. If the host returns a "port unreachable" message, that port is considered closed. This method can be time consuming because most UNIX hosts limit the rate of ICMP errors. Fortunately, Nmap detects this rate and slows itself down, so not to overflow the target with messages that would have been ignored. Launch a UDP scan as follows:

# nmap -sU 10.0.0.1

WARNING:  -sU is now UDP scan -- for TCP FIN scan use -sF

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)

Interesting ports on saturnlink.nac.net (10.0.0.1):

Port    State       Protocol  Service

53      open        udp        domain

111     open        udp        sunrpc

123     open        udp        ntp

137     open        udp        netbios-ns

138     open        udp        netbios-dgm

177     open        udp        xdmcp

1024    open        udp        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds

3.3 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.

# nmap -sS -O 10.0.0.1

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)

Interesting ports on comet (10.0.0.1):

Port    State       Protocol  Service

7       open        tcp        echo

9       open        tcp        discard

13      open        tcp        daytime

19      open        tcp        chargen

21      open        tcp        ftp

...

TCP Sequence Prediction: Class=random positive increments

                         Difficulty=17818 (Worthy challenge)

Remote operating system guess: Solaris 2.6 - 2.7

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds

The TCP Sequence Prediction tells us how difficult TCP sequence number prediction is for the remote host. This is valuable to an attacker looking for hosts that can be vulnerable to session hijacking.

3.4 Other Options

Enter the **-oN<textfile name> t**o create a human readable output file:

#nmap -sT -O -oN sample.txt 10.0.0.0-50

Enter the **-oM <textfile name>** to pipe the output into a machine parsable file:

#nmap -sT -O -oM sample.txt 10.0.0.0-50

**-P0**    Do  not  try  to  ping  hosts at all before scanning them.  Since Nmap will ping a target with both TCP "ping" and ICMP echo before attempting a port scan, sites blocking ICMP and TCP probes will not be scanned by default.

**"-v"**  a verbose option that can be used with all types of scans. You can use this flag once, **even twice**, to get more information about the target's machine.

The ability to target specific ports is accomplished with the **"-p "** option. For instance, if an attacker wanted to probe your webserver for ftp (port 21), telnet (port 23), name service (port 53), and http (port 80), and wanted to know the OS you were using, he/she may try the SYN scan:

# nmap -sS -p 21,23,53,80 -O -v 10.6.1.10

For a complete list of the options for Nmap, you can see the manual of the NMAP in website <http://www.insecure.org/nmap>.

4. Quickstart of Nmap

4.1 Ping Sweeping

Icmp ping                     # nmap -sP 10.0.0.0/24

tcp ping                      # nmap -sP -PT80 10.0.0.0/24

4.2 Port Scanning

TCP connect                # nmap -sT 10.0.0.1

Stealth Scanning           # nmap -sS 10.0.0.1

UDP Scanning             # nmap -sU 10.0.0.1

Stealth FIN                  # nmap -sF 10.0.0.1

Xmas Tree                   # nmap -sX 10.0.0.1

Null scan.                    # nmap -sN 10.0.0.1

4.3 OS Fingerprinting   # nmap -sS -O 10.0.0.1

 References:

 1. �Scanning and Defending Networks with Nmap� By Rich Jankowski 6/27/2002 <http://www.linuxsecurity.com/feature_stories/feature_story-4.html>

2. �Tools of the Trade: nmap� By Josh Flechtner

<http://www.linuxgazette.com/issue56/flechtner.html>

3. Manual of NMAP

<http://www.insecure.org/nmap/data/nmap_manpage.html>