**Step by Step Instructions**

Take the following steps after you successfully log on to the Window XP Virtual Machine:

type◊ Run ◊1. You can click Start  **cmd** to access the command prompt. Then type **ipconfig** to verify that the IP address is 192.168.100.104. Commands for nmap may be entered through the command prompt. You may want to type **nmap -h** to see various nmap options. If you wish to cancel a scan while in the command prompt, press the 'ctrl' key plus the 'c' key.

2. You may wish to click on the Zenmap icon for the graphical front end.

3. In the Zenmap “Target” field, you will type the name of the target host, there are three targets and **you are to scan one at a time**: 192.168.100.103, 192.168.100.105, 192.168.100.106. You will see this entry appear in the “Command” field. You can modify the command as appropriate, to try out different scans by using the 'scan' button. You can cancel a scan by clicking the cancel button.

4. From either the Zenmap Graphical frontend, or the command line, you will type in the nmap command with various option(s) and target(s).

**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 in our case we can indicate the range of target hosts as follows: **192.168.100.103-106**

**A) Which hosts are up now?   “Ping Sweeping”**

Intruders can sweep entire networks to locate 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, we could scan all hosts on the 192.168.100.0 network.

**# nmap -sP 192.168.100.\***

(Both Zenmap and the command-line will allow you to enter this command and run the scan, but Zenmap, due to a software glitch, will change the displayed command-line in the output area to “nmap -sn 192.168.100.\*”; if you run the command in Zenmap, just ignore the display glitch; Note the results.)

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 192.168.100.\***

(Both Zenmap and the command-line will allow you to enter this command and run the scan, but Zenmap, due to a software glitch, will change the displayed command-line in the output area to “nmap -sn -PA80 192.168.100.\*”; if you run the command in Zenmap, just ignore the display glitch; Note the results.)

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

**B) 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.

**C) 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 192.168.100.103-106**

**D) 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, which could be obtained by trying "su -" command at the knoppix prompt.** The "-sS" flag will launch a SYN scan against a host or network as:

**# nmap -sS 192.168.100.103-106**

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 noncompliance with TCP standards, the FIN, Xmas Tree, and Null scans are only effective on non-Microsoft operating systems.***

**E) 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 192.168.100.103, 192.168.100.105, 192.168.100.106**

**F) 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 192.168.100.103-106**

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.

**G) Other Options**

**-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 192.168.100.103**

**“-iR”** Use this command to instruct nmap to scan random hosts.

**A) Ping Sweeping**

Icmp ping                     # nmap -sP “host IP address”

tcp ping                        # nmap -sP -PT80 “host IP address”

**B) Port Scanning**

TCP connect                # nmap -sT “host IP address”

Stealth Scanning           # nmap -sS “host IP address”

UDP Scanning             # nmap -sU “host IP address”

Stealth FIN                  # nmap -sF “host IP address”

Xmas Tree                   # nmap -sX “host IP address”

Null scan.                     # nmap -sN “host IP address”

**C)** **OS Fingerprinting**   # nmap -sS -O “host IP address”