CSC 433 NMap Lab Exercise Lab for Stimulus and Response

Instructions: Please complete each Task in section 3 but do not record the output of each task. Once the tasks are completed, answer questions 1 through 3 and post your answers to the assignment.

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. The tasks you need to complete are highlighted. After completing all the tasks, please answer questions 1 through 3. You may need to revisit some of the commands you use in this lab to answer the questions.

2. Introduction NMAP

In order to access 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 is able to sweep networks and look for 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.

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 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 10.123.10.*, which is the same as 10.123.10.0/24.

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.

Task: scan a host.

```
nmap -sP scanme.nmap.org
```

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 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.**

Task: Launch the TCP ping sweep scan as follows:

```
nmap -sP -PT80 scanme.nmap.org
```

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, 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.

Task: Perform a TCP connect scan is used with the "-sT" flag as:

nmap -sT scanme.nmap.org (will probably take too long, try it just for a few ports with the –p option. E.g., -p 21-25, 80,139)

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.

Task: Use the "-sS" flag to launch a SYN scan against a host:

```
nmap -sS scanme.nmap.org
```

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.

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.

Task: Launch a UDP scan as follows:

nmap –sU scanme.nmap.org (will probably take too long, try it just for a few ports with the –p option. E.g., -p 53)

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.

Task: Determine the operating system of a host:

nmap -sS -O scanme.nmap.org

4. Lab Questions (Turn in the answers to these questions)

1.) What is the IP of scanme.nmap.org?

2.) If you found a computer that is up and running, which services (TCP and UDP) are open on it?

3.) Can you determine the Operating system and its possible version that is running on any of the live computers?