CPTR 427 Lab #3 Name

Port Scanning with NMAP

# Research Questions:

1. What is a stealth scan?
2. What legitimate reason might you have for using a stealth scan?
3. What is the name of the most popular scanner?
4. What is a Christmas tree scan and will windows respond to it?
5. What legitimate (and lazy) reason might a system admin use a port scanner?
6. What is TCP finger printing?

# Lab OPs

Network and OS updates

1. Install nmap (the most popular and free) network scanner on your Linux system.

# Demos

Demo each of the following in a separate session. When you are satisfied that each command is working correctly, show the annotated sessions to Dr. A. Each session should have the command written at the top and then the output of the command below**. For example**:

# Scan 1. Run a SYN scan (the default for nmap) against the firewall/gateway

# Command: **nmap –sS –oN scan1.txt sec-fire.cs.southern.edu**

Starting Nmap 4.20 ( http://insecure.org ) at 2008-02-04 14:22 EST

Interesting ports on 10.0.0.1:

Not shown: 1696 filtered ports

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:40:33:D4:01:35 (Addtron Technology CO.)

Nmap finished: 1 IP address (1 host up) scanned in 23.740 seconds

**Answer any questions after the required scan in the space provided. For some of these questions you will have to team up with a partner. You will scan his computer and he will scan yours.**

1. Perform a ping sweep of the 192.168.37.0 network. How many systems responded?
2. Determine open tcp and udp ports on a partner’s computer. List the differences between your two computers.
3. Identify the operating system of your partners computer. What did nmap indicate?
4. Use the time command (man time to see the syntax for the command) to determine the effects of –T0 and –T5. Summarize the difference in running times. Now compare them to the Aggressive template.

1. Perform FIN, NULL and XMAS scans and compare your output of each. Are the different? If so why?

1. Finally, time an aggressive (advanced), verbose scan of your partners system. Give the time results: