Vulnerability testing with Nmap

Work in groups of **two**.

Goal: To learn how to use nmap as a vulnerability testing tool.

Part 1: Configure one nmap.

a) Download and install nmap from www.insecure.org.
b) Try #man nmap
c) Scan your own host.
d) Scan your partner's host.
e) Scan the entire 192.168.208.x subnet.

Part 3: Hardening.

Based on your scan results, further harden you system so that only the ssh and ftp ports are open. Describe what you do.

Part 2: Questions

1) In light of the security hardening you did last week, do you feel your computer is secure from unwanted connections?

2) Is your partners host secure from unwanted connections?

3) What is the general state of security in the room based on your scan?

Usage: nmap [Scan Type(s)] [Options] <host or net list>
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'

Some Common Scan Types ('*' options require root privileges):

-sT TCP connect() port scan (default)

* -sS TCP SYN stealth port scan (best all-around TCP scan)

* -sU UDP port scan

-sP ping scan (Find any reachable machines)

* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)

-sR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

* -O Use TCP/IP fingerprinting to guess remote operating system

-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'

-F Only scans ports listed in nmap-services

-v Verbose. Its use is recommended. Use twice for greater effect.

-P0 Don't ping hosts (needed to scan www.microsoft.com and others)

* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy

-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]

-oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>

-iL <inputfile> Get targets from file; Use '-' for stdin

* -S <your_IP>/-e <devicename> Specify source address or network interface