Download and install nmap. ([www.nmap.org](http://www.nmap.org))

Read through this entire section first! We are going to nmap a small local network, ideally your home network. If you don’t have/use a home network, visit a coffee shop. First, you should determine the IP address range used for the network being scanned. If you are working with your home network, you can log in to the router and see what block it is assigning. The most likely candidates will be 192.168.x.x, many routers will use 192.168.0.0/24 or 192.168.1.0/24. If you can’t determine your IP range, check your system and find its current address (using ipconfig if Windows, etc.). Use the first 3 octets, then .0/24.

Before scanning, answer the following:

1. Are you scanning a private (home) or public (coffee shop) IP space:
2. What is the IP range you are scanning:
3. If you are at home and using your router for IP information, dump the active IP table as well. (This varies by router manufacturer).

Put in the network block to scan (e.g., 192.168.1.0/24) and select the “Quick scan plus” option. Run the scan. It may take a few minutes, be patient.

1. How many systems did the scan find?
2. Is there anything found you didn’t expect?
3. If you have the router active list, how does the nmap list compare?
4. What information about each target did the Quick scan plus return?

Now run the scan again as an “Intense scan”.

1. What information does the intense scan give you that Quick scan plus did not?
2. From the scan data obtained so far, can you identify every device found in the scans?

This question is 10 of the 25 points:

For an unknown device, what steps can you take to determine what (and where) it is?

Hints:

* Try putting the MAC address in to: <https://macvendors.com/>. If you don’t have any “unknown” devices, pick something that isn’t a PC and try its MAC at the web site.
* What ports does the device use?
* Are there other scan options that could help?