Using nmap

Network Scanning

* # nmap 192.168.1.0/24 -sP -oA 131210\_NetScan (old)
* # nmap 192.168.1.0/24 -sn -oA 131210\_NetScan (new)

Host Port Scan

* Default Scan/SYN Scan/Half-Open Scan/Stealth Scan
	+ > SYN >| < SYN/ACK < | > RST >
	+ # nmap 192.168.1.125
	+ # nmap 192.168.1.125 -sS
* Connect Scan, TCP Scan, Vanilla Scan
	+ Most reliable, some say it is the fastest.
	+ > SYN >| < SYN/ACK < | > ACK > | > RST/ACK >
	+ # nmap 192.168.1.125 -sT
	+ # nmap 192.168.1.125 -sT -r -T5
	+ # nmap 192.168.1.125 -sT -p 0-65535 -r -T5
	+ # nmap 192.168.1.125 -sT -p- -r -T5

Host Service Scan

* # nmap 192.168.1.125 -p 80 -sV

**Other Scans**

**UDP Scan**

* Open Port
* # nmap 192.168.1.125 -sU -p 138
	+ No reply from target
* Closed Port
* # nmap 192.168.1.125 -sU -p 111

Operating System Scan

* # nmap 192.168.1.125 -O

Aggressive Scan

* # nmap 192.168.1.125 -A
* # nmap 192.168.1.125 -A -p-
* # nmap 192.168.1.125 -A -p- -T5 -r