Hacking

Assignment: Try the following

BASIC SCAN

nmap [ip one] [ip two] [ip three] ...

nmap 192.168.3.17-30 // an ip range

nmap 192.168.3.* // all 255 address

nmap -iL target.txt // import from List/file

AGRESSIVE SCAN

nmap -A [ip address/domain nam]

nmap --traceroute [ip address/domain nam]

nmap -O [ip address/domain nam] //operating system

nmap -sV [ip address/domain nam] //Version of the services that are running

-F = fast scan //scans only about 1000

-p = to give it a port or a range 20-25

nmap -p 20-25,80,443 [ip address/domain nam] //scan specific ports

nmap -p http,mysql [ip address/domain nam] //scan ports by names

nmap -p- [ip address/domain nam] //scans every possible port // takes a looooong tim

nmap --open [ip address/domain nam] // scans only the open ports

Saving scan results to a file

nmap -F -oN Desktop/results.txt [ip address/domain nam] //N for saving in regular Text file //X for xml format

nmap -v [ip address/domain nam] //verbos