Nmap

Scan a single host or an IP address

Scan a single ip address
>nmap 192.168.1.1

Scan a host name
>nmap www.walla.co.il

Scan a host name with more info
>nmap –v www.walla.co.il

Show host interfaces and routes

>namp --iflist

perform a fast scan

>nmap –F 192.168.1.1

Scan multiple IP address or subnet

>nmap 192.168.1.1 192.168.1.25 192.168.1.31

>namp 192.168.1.1 – 20

>nmap 192.168.1.*

>namp 192.168.1.0/24

Excluding hosts/networks

>nmap 192.168.1.0/24 --exclude 192.168.1.5
>nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254

detect remote operating system

>nmap -O 192.168.1.1
>nmap -O --osscan-guess 192.168.1.1
>nmap -v -O --osscan-guess 192.168.1.1

Find out if a host/network is protected by a firewall

>nmap -sA 192.168.1.254
>nmap -sA www.walla.co.il

Scan a host when protected by the firewall

>nmap -PN 192.168.1.1
>nmap -PN www.walla.co.il

Scan a firewall for security weakness

TCP Null Scan to fool a firewall to generate a response
>nmap -sN 192.168.1.254

TCP Fin scan to check firewall
>nmap -sF 192.168.1.254

TCP Xmas scan to check firewall
Sets the FIN, PSH, and URG flags, lighting the packet up
>nmap -sX 192.168.1.254

Scan a network and find out which servers and devices are running

>nmap -sP 192.168.1.0/24

Only show open (or possibly open) ports

>nmap --open 192.168.1.1
>nmap --open www.walla.co.il

Show all packets sent and received

>nmap --packet-trace 192.168.1.1
>nmap --packet-trace www.walla.co.il

save output to a text file

>nmap 192.168.1.1 > output.txt