nmap Cheat Sheet

by deassain via cheatography.com/1677/cs/538/

nmap

-O

Tries to detect the used operating system

-oA

This outputs the scan into all possible output files

-sN

This is a TCP Null scan. (Ping sweep)

-PN

Don't do host discovery, just treat every host as online

--reason

Display port state reason

--max-retry

maximum times nmap should retry to communicate to a host.

--top-ports

Top ports is to limit the amount of ports to scan.

-T

Sets the aggressiveness (1 to 5) of nmap

-sSV

TCP scan

-sUV

UDP scan

-p-

All ports

-iL

Accepts a path to an input file of IP addresses

TCPdump/Windump

-nn

Do not resolve hostnames

-p

Do not put it into promiscious mode

-s

Snapshot length

-i

Interface number

-w

Write to file, option followed by path

Common Win/TCP dump commands

windump -nn -p -s0 -i *interface* **-w** */path/to/-dumpfolder/client_InternalorExternal_da-te.pcap*

tcpdump -nn -p -s0 -i *interface* **-w** */path/to/-dumpfolder/client_InternalorExternal_da-te.pcap*

Common Nmap Commands

nmap -sN -oA *nmap_sN_range range*

nmap -sSV -- reason --top-ports 2000 -O -PN -oA *nmap_sSV_top2000_iprange iprange*

nmap -sSV --reason --top-ports 2000 -O -iL *input* **-oA** *nmap_sSV_top2000_iprange-_scan2*

nmap -sUV -- reason --top-ports 500 -O -PN -oA *nmap_sUV_top500_iprange iprange*

nmap -sUV --reason --top-ports 500 -O -iL *input* **-oA** *nmap_sSV_top500_iprange_-scan2*