

### 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 promiscuous 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\_date.pcap**

**tcpdump -nn -p -s0 -i interface -w /path/to/dumpfolder/client\_InternalorExternal\_date.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**



By deassain

[cheatography.com/deassain/](http://cheatography.com/deassain/)

Not published yet.

Last updated 12th May, 2016.

Page 1 of 1.

Sponsored by [CrosswordCheats.com](http://CrosswordCheats.com)

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>