

Number of Ports on a Computer

65,535 ports

Port Statuses

Open Closed Filtered (*Firewall*)

Usual Ports (TCP/UDP)

HTTP	80
HTTPS	443
Windows NETBIOS	139
SMB	445
SMTP	587 or 25 (old)
RDP	3389
FTP	20 & 21
SSH	22
DNS	53

Trivia

How are Network Connections made?

Network connections are made between two ports – an open port listening on the server and a randomly selected port on your own computer.

Source:

[Here](#)

Nmap Basic Commands

nmap nmap's help menu

-h

man nmap's manual

nmap

nmap Syn Scan

-Ss

-sU UDP Scan

-p 80 Scans only port 80 (*used as an instance obviously*)

-sV Detects scanned Service Version

-v // -vv Increases verbosity level (greater output - recommended)

-oA Saves the nmap results in three major formats

-oN Save the output in a normal format

Nmap Basic Commands (cont)

- Saves the output on a Grepable

oG format

-a Agressive Mode (*very Loud - activates service detection, operating system detection, a traceroute and common script scanning*)

-t5 Increases timing template (*0-5, louder and faster but with more errors*)

-O Detects OS

-p Defines port range (*instance: 80 to 100*)

100

-p- Scans all ports

