Nmap Basics Cheat Sheet Cheat Sheet

by Geringonça (akirasett) via cheatography.com/185306/cs/39035/

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 -h	nmap's help menu
man nmap	nmap's manual
nmap -Ss	Syn Scan
-sU	UDP Scan
-p 80	Scans only port 80 *(used as an instance obviously)*
-sV	Detects scanned Service Version
-v // -vv	Increses 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)

-oG	Saves the output on a Grepable format
-a	Agressive Mode *(very Loud - activates service detection, operating system detection, a traceroute and common script scanning)*
-t5	Increses timing template *(0-5, louder and faster but with more errors)*
-O	Detects OS
-p 80-100	Defines port range *(instance: 80 to 100)*
-p-	Scans all ports