netcat cheat sheet

comparitech

Installation / Run Modes

Client Mode	**Connect to a host located anywhere**
Client Mode Syntax	`nc options hostname port[1] port[2]...`
Server Mode	**Listen for incoming connections**
Server Mode Syntax	`nc -l -p port [hostname] [port]`

Netcat Command Flags

Option	Description	Example
-h	Help	nc -h
-z (host name)(port range)	Port scan for a host or IP address	nc -z 10.1.1.1 1-100
-v	Verbose scan	nc -z -v 10.1.1.1 1-100
-n	Fast scan by disabling DNS resolution	nc -z -n 10.1.1.1 1-100
-l	TCP server mode	nc -l -p 50
>	Server file redirection	netcat -l -p 1000 > scan.txt
<	Client file redirection	nc 10.1.1.1 1000 < scan.txt
-k	Listen to port & IP address after connection close	nc -k -l 1000
-w	Define timeout value	nc -w 180 10.1.1.1 2222
-4	IPv4 only	nc -4 -l 1000
-6	IPv6 only	nc -6 -l 1000