```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 1234 -c "/bin/sh"
```
(primo terminale)

-l: Netcat si mette in **modalità ascolto** sulla macchina locale

-p 1234: Netcat ascolta sulla porta **1234** per le connessioni in ingresso

-c “/bin/sh”: Quando qualcuno si connette alla porta 1234, Netcat avvia una shell /bin/sh sulla macchina di ascolto, permettendo al client remoto di interagire con la shell del sistema.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234
```

comando usato in un altro terminale per connettersi ed eseguire in shell , così da usare i comandi in questo secondo terminale e avere tutte le informazioni necessarie da remoto

```
sudo su
whoami
root
```

perchè ho eseguito sudo su nel secondo terminale e quindi dando conferma nel primo terminale siamo root anziché kali

```
ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.7  23632 14464 ?        Ss   09:40   0:00 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    09:40   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    09:40   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   09:40   0:00 [kworker/R-kvfree_rcu_reclaim]
root           5  0.0  0.0      0     0 ?        I<   09:40   0:00 [kworker/R-rcu_gp]
root           6  0.0  0.0      0     0 ?        I<   09:40   0:00 [kworker/R-sync_wq]
```

sempre dal secondo terminale

```
uname -a
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64 GNU/Linux
```

whoami: Mostra il nome dell'utente che ha eseguito il comando

ps- aux: Mostra tutti i processi in esecuzione nel sistema, con dettagli come l'ID del processo, l'utente che lo ha avviato e l'uso delle risorse

uname -a: Fornisce informazioni dettagliate sul sistema operativo e la macchina in uso, come la versione del kernel e l'architettura

```
┌──(root㉿kali)-[/home/kali]
└─# nc -l -p 1234 -c "whoami"
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234
root
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -l -p 1234 -c "uname -a"
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64 GNU/Linux
```

```
┌──(root㉿kali)-[/home/kali]
└─# nc -l -p 1234 -c "ps -aux"
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.100 1234
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.7  23632 14464 ?        Ss   09:40   0:00 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    09:40   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    09:40   0:00 [pool_workqueue_release]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 12:48 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000064s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 12:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00028s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:CC:EB:61 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.50.101 -p 1-1024
```

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      36898/udp   mountd
|   100005  1,2,3      59684/tcp   mountd
|   100021  1,3,4      44462/tcp   nlockmgr
|   100021  1,3,4      55670/udp   nlockmgr
|   100024  1          34127/udp   status
|_  100024  1          49372/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

-sS: SYN scan, metodo meno invasivo rispetto a -sT, invia un pacchetto **SYN** (come se volesse iniziare una connessione TCP) se la porta risponde con **SYN-ACK**, Nmap sa che la porta è **aperta**, e invia un **RST** per chiudere subito la connessione, senza completarla. Se riceve un **RST**, la porta è **chiusa**.

-sT: metodo più invasivo rispetto a -sS, Usa le normali chiamate di sistema del sistema operativo, stabilendo una connessione completa come farebbe un browser o qualsiasi programma. In quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

-A: è il più aggressivo, ci permette di avere molte informazioni sul target, come:
- Esegue una **scansione delle porte**.
- Esegue una **fingerprint del sistema operativo** (OS detection).
- Tenta di identificare **versioni dei servizi** in esecuzione.
- Esegue **traceroute**.
- Include alcuni **script NSE** di Nmap per raccogliere ulteriori info.