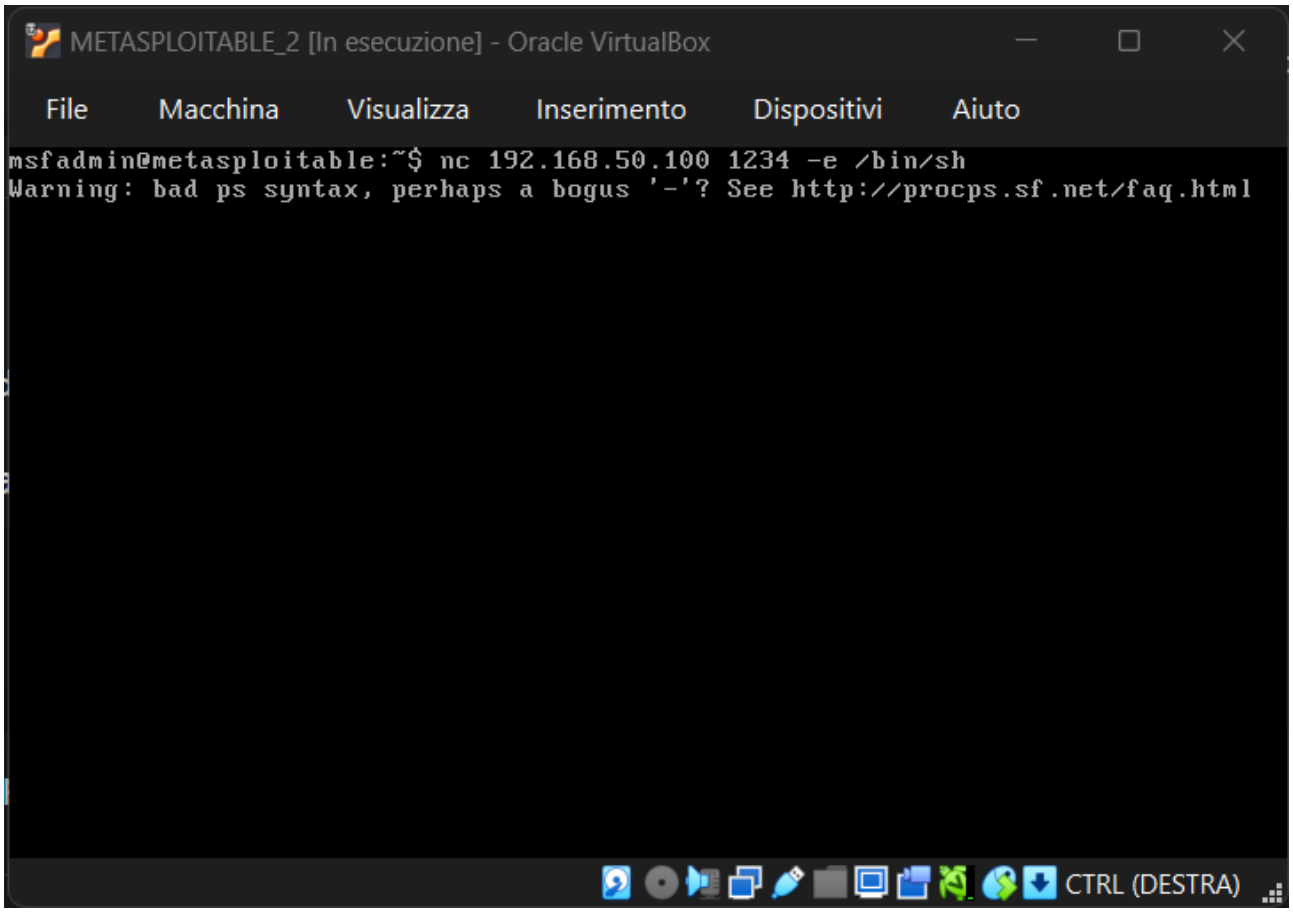
PARTE 1

```
┌──(pireddone㉿kali)-[~]
└─$ nc.traditional -l -p 1234
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.3   2844  1692 ?        Ss   15:03   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   15:03   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   15:03   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   15:03   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   15:03   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   15:03   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   15:03   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   15:03   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   15:03   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   15:03   0:00 [kacpi_notify]
root        90  0.0  0.0      0     0 ?        S<   15:03   0:00 [kseriod]
root       128  0.0  0.0      0     0 ?        S    15:03   0:00 [pdflush]
root       129  0.0  0.0      0     0 ?        S    15:03   0:00 [pdflush]
root       130  0.0  0.0      0     0 ?        S<   15:03   0:00 [kswapd0]
root       172  0.0  0.0      0     0 ?        S<   15:03   0:00 [aio/0]
root      1128  0.0  0.0      0     0 ?        S<   15:03   0:00 [ksnapd]
root      1296  0.0  0.0      0     0 ?        S<   15:03   0:00 [ata/0]
root      1300  0.0  0.0      0     0 ?        S<   15:03   0:00 [ata_aux]
root      1311  0.0  0.0      0     0 ?        S<   15:03   0:00 [scsi_eh_0]
root      1314  0.0  0.0      0     0 ?        S<   15:03   0:00 [scsi_eh_1]
root      1334  0.0  0.0      0     0 ?        S<   15:03   0:00 [ksuspend_usbd]
root      1336  0.0  0.0      0     0 ?        S<   15:03   0:00 [khubd]
root      2064  0.0  0.0      0     0 ?        S<   15:03   0:00 [scsi_eh_2]
root      2268  0.0  0.0      0     0 ?        S<   15:03   0:00 [kjournald]
root      2422  0.0  0.1   2092   620 ?        S<s  15:03   0:00 /sbin/udevd --daemon
```



PARTE 2

Scan Well-know

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -sT -p 1-1024 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 21:23 CET
Nmap scan report for 192.168.50.101
Host is up (0.0073s 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:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds
```

Scan Syn

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -sS -p 1-1024 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 21:25 CET
Nmap scan report for 192.168.50.101
Host is up (0.00076s 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:C7:D0:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.02 seconds
```

Scan Switch -A

```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:C7:D0:E5 (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

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-12-02T15:27:46-05:00
|_clock-skew: mean: 2h29m57s, deviation: 3h32m07s, median: -2s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   1.42 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 90.58 seconds
```

```
┌──(pireddone㉿kali)-[~]
└─$ nmap -A -p 1-1024 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 21:26 CET
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
Not shown: 1012 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
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
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      37266/udp   mountd
|   100005  1,2,3      52899/tcp   mountd
|   100021  1,3,4      40454/tcp   nlockmgr
|   100021  1,3,4      49470/udp   nlockmgr
|   100024  1          51495/tcp   status
|_  100024  1          52060/udp   status
```