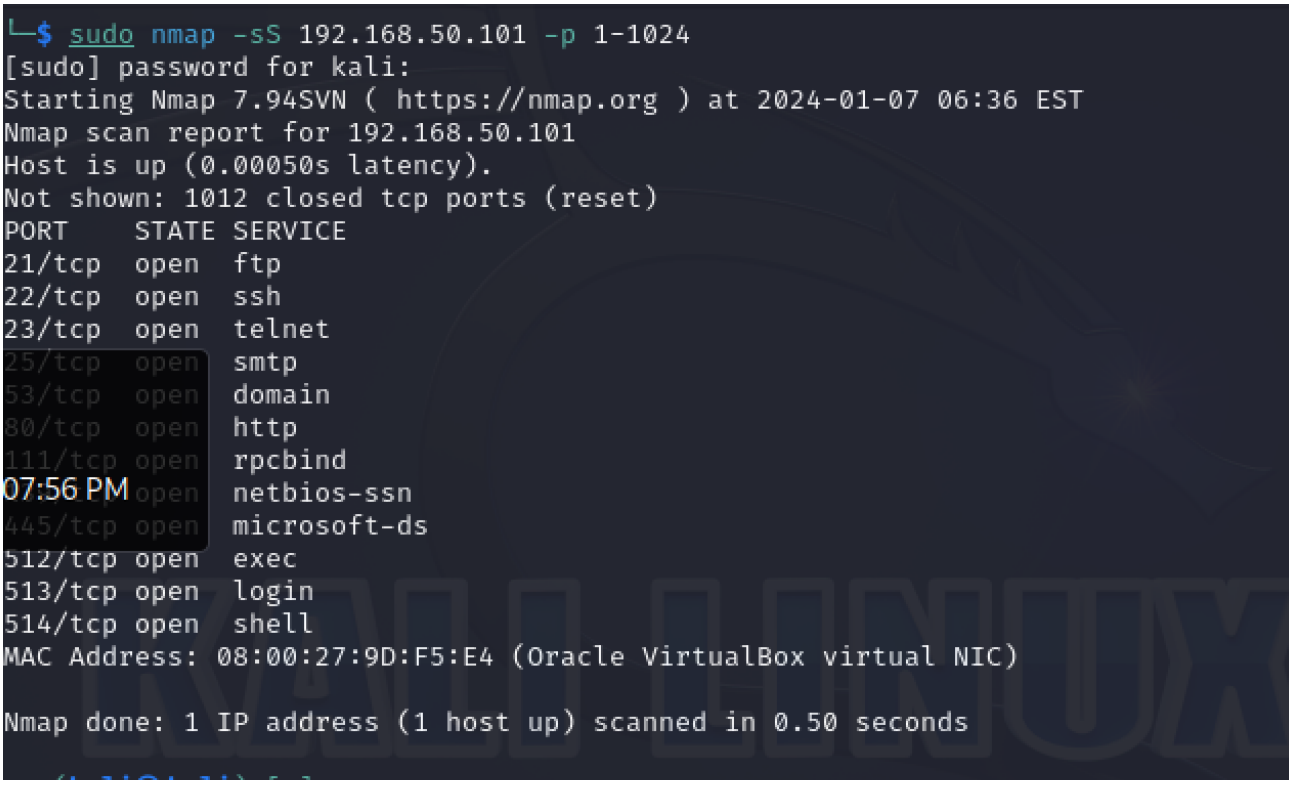
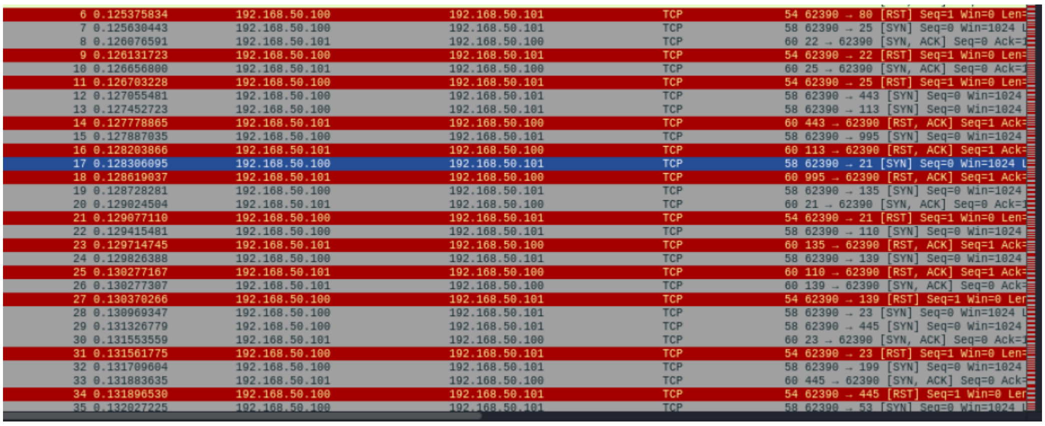
NMAP

Comando -sS dove non si conclude il three hand shake.
Infatti avremo solo SYN, SYN-ACK come si può vedere da scansione Wireshark in basso

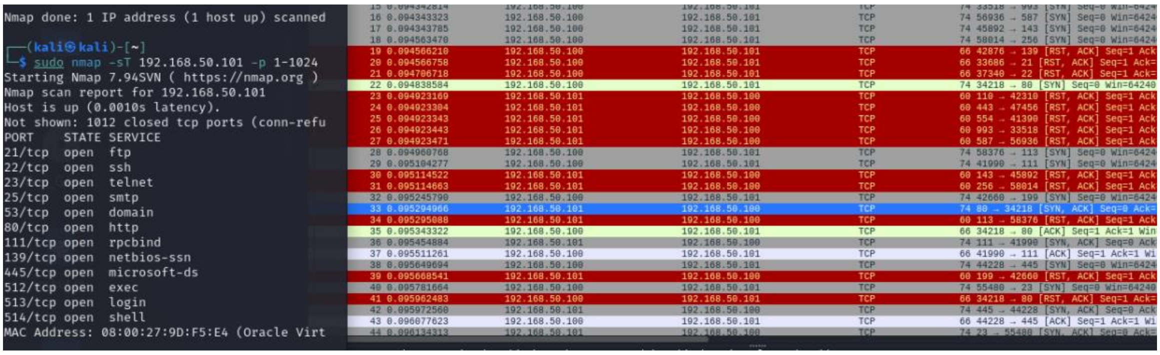


```
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-07 06:36 EST
Nmap scan report for 192.168.50.101
Host is up (0.00050s latency).
Not shown: 1012 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
07:56 PM open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
MAC Address: 08:00:27:9D:F5:E4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```



```
 6 0.125375834   192.168.50.100   192.168.50.101   TCP   54 62390 → 80 [RST] Seq=1 Win=0 Len=
 7 0.125630443   192.168.50.100   192.168.50.101   TCP   58 62390 → 25 [SYN] Seq=0 Win=1024 L
 8 0.126076591   192.168.50.101   192.168.50.100   TCP   60 22 → 62390 [SYN, ACK] Seq=0 Ack=1
 9 0.126131723   192.168.50.100   192.168.50.101   TCP   54 62390 → 22 [RST] Seq=1 Win=0 Len=
10 0.126656800   192.168.50.101   192.168.50.100   TCP   60 25 → 62390 [SYN, ACK] Seq=0 Ack=1
11 0.126703228   192.168.50.100   192.168.50.101   TCP   54 62390 → 25 [RST] Seq=1 Win=0 Len=
12 0.127055481   192.168.50.100   192.168.50.101   TCP   58 62390 → 443 [SYN] Seq=0 Win=1024
13 0.127452723   192.168.50.100   192.168.50.101   TCP   58 62390 → 113 [SYN] Seq=0 Win=1024
14 0.127778865   192.168.50.101   192.168.50.100   TCP   60 443 → 62390 [RST, ACK] Seq=1 Ack=
15 0.127887035   192.168.50.100   192.168.50.101   TCP   58 62390 → 995 [SYN] Seq=0 Win=1024
16 0.128203866   192.168.50.101   192.168.50.100   TCP   60 113 → 62390 [RST, ACK] Seq=1 Ack=
17 0.128306095   192.168.50.100   192.168.50.101   TCP   58 62390 → 21 [SYN] Seq=0 Win=1024 L
18 0.128619037   192.168.50.101   192.168.50.100   TCP   60 995 → 62390 [RST, ACK] Seq=1 Ack=
19 0.128728281   192.168.50.100   192.168.50.101   TCP   58 62390 → 135 [SYN] Seq=0 Win=1024
20 0.129024504   192.168.50.101   192.168.50.100   TCP   60 21 → 62390 [SYN, ACK] Seq=0 Ack=1
21 0.129077110   192.168.50.100   192.168.50.101   TCP   54 62390 → 21 [RST] Seq=1 Win=0 Len=
22 0.129415481   192.168.50.100   192.168.50.101   TCP   58 62390 → 110 [SYN] Seq=0 Win=1024
23 0.129714745   192.168.50.101   192.168.50.100   TCP   60 135 → 62390 [RST, ACK] Seq=1 Ack=
24 0.129826388   192.168.50.100   192.168.50.101   TCP   58 62390 → 139 [SYN] Seq=0 Win=1024
25 0.130277167   192.168.50.101   192.168.50.100   TCP   60 110 → 62390 [RST, ACK] Seq=1 Ack=
26 0.130277307   192.168.50.101   192.168.50.100   TCP   60 139 → 62390 [SYN, ACK] Seq=0 Ack=
27 0.130370266   192.168.50.100   192.168.50.101   TCP   54 62390 → 139 [RST] Seq=1 Win=0 Ler
28 0.130969347   192.168.50.100   192.168.50.101   TCP   58 62390 → 23 [SYN] Seq=0 Win=1024 L
29 0.131326779   192.168.50.100   192.168.50.101   TCP   58 62390 → 445 [SYN] Seq=0 Win=1024
30 0.131553559   192.168.50.101   192.168.50.100   TCP   60 23 → 62390 [SYN, ACK] Seq=0 Ack=1
31 0.131561775   192.168.50.100   192.168.50.101   TCP   54 62390 → 23 [RST] Seq=1 Win=0 Len=
32 0.131709604   192.168.50.100   192.168.50.101   TCP   58 62390 → 199 [SYN] Seq=0 Win=1024
33 0.131883635   192.168.50.101   192.168.50.100   TCP   60 445 → 62390 [SYN, ACK] Seq=0 Ack=
34 0.131896530   192.168.50.100   192.168.50.101   TCP   54 62390 → 445 [RST] Seq=1 Win=0 Ler
35 0.132027225   192.168.50.100   192.168.50.101   TCP   58 62390 → 53 [SYN] Seq=0 Win=1024 L
```

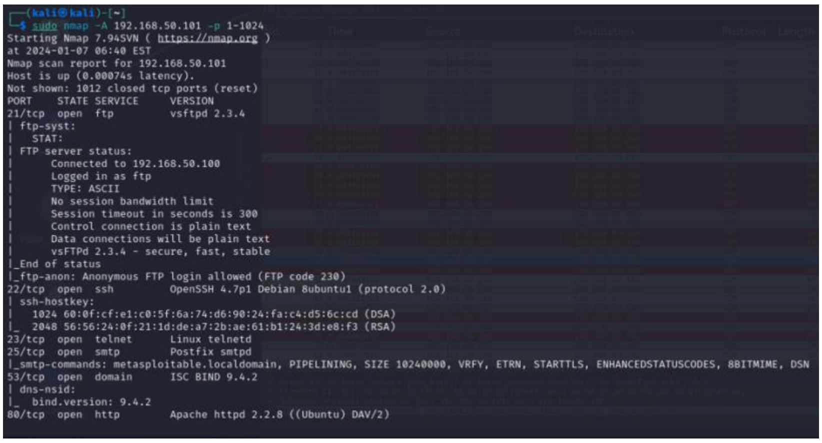
Comando -sT
Più invasivo rispetto a -sS



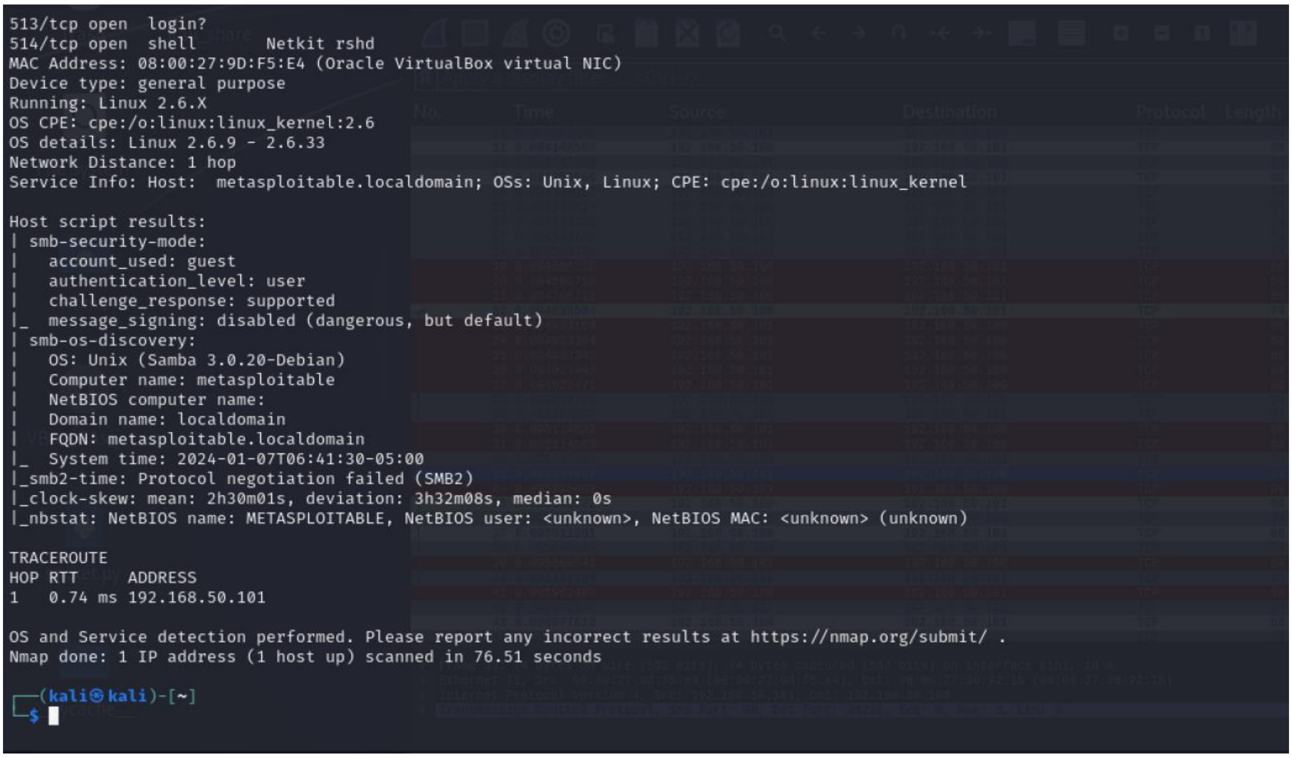
```
Nmap done: 1 IP address (1 host up) scanned

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 1012 closed tcp ports (conn-refu
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: 08:00:27:9D:F5:E4 (Oracle Virt
```

```
15 0.094342814   192.168.50.100   192.168.50.101   TCP   74 33518 → 993 [SYN] Seq=0 Win=6424
16 0.094343323   192.168.50.100   192.168.50.101   TCP   74 56936 → 587 [SYN] Seq=0 Win=6424
17 0.094343785   192.168.50.100   192.168.50.101   TCP   74 45892 → 143 [SYN] Seq=0 Win=6424
18 0.094563470   192.168.50.100   192.168.50.101   TCP   74 58014 → 256 [SYN] Seq=0 Win=6424
19 0.094566210   192.168.50.100   192.168.50.101   TCP   66 42876 → 139 [RST, ACK] Seq=1 Ack
20 0.094566758   192.168.50.100   192.168.50.101   TCP   66 33686 → 21 [RST, ACK] Seq=1 Ack=
21 0.094706718   192.168.50.100   192.168.50.101   TCP   66 37340 → 22 [RST, ACK] Seq=1 Ack=
22 0.094838584   192.168.50.100   192.168.50.101   TCP   74 34218 → 80 [SYN] Seq=0 Win=64240
23 0.094923169   192.168.50.101   192.168.50.100   TCP   60 110 → 42310 [RST, ACK] Seq=1 Ack
24 0.094923304   192.168.50.101   192.168.50.100   TCP   60 443 → 47456 [RST, ACK] Seq=1 Ack
25 0.094923343   192.168.50.101   192.168.50.100   TCP   60 554 → 41390 [RST, ACK] Seq=1 Ack
26 0.094923443   192.168.50.101   192.168.50.100   TCP   60 993 → 33518 [RST, ACK] Seq=1 Ack
27 0.094923471   192.168.50.101   192.168.50.100   TCP   60 587 → 56936 [RST, ACK] Seq=1 Ack
28 0.094960768   192.168.50.100   192.168.50.101   TCP   74 58376 → 113 [SYN] Seq=0 Win=6424
29 0.095104277   192.168.50.100   192.168.50.101   TCP   74 41990 → 111 [SYN] Seq=0 Win=6424
30 0.095114522   192.168.50.101   192.168.50.100   TCP   60 143 → 45892 [RST, ACK] Seq=1 Ack
31 0.095114663   192.168.50.101   192.168.50.100   TCP   60 256 → 58014 [RST, ACK] Seq=1 Ack
32 0.095245790   192.168.50.100   192.168.50.101   TCP   74 42660 → 199 [SYN] Seq=0 Win=6424
33 0.095294966   192.168.50.101   192.168.50.100   TCP   74 80 → 34218 [SYN, ACK] Seq=0 Ack=
34 0.095295088   192.168.50.101   192.168.50.100   TCP   60 113 → 58376 [RST, ACK] Seq=1 Ack
35 0.095343322   192.168.50.100   192.168.50.101   TCP   66 34218 → 80 [ACK] Seq=1 Ack=1 Win
36 0.095454884   192.168.50.101   192.168.50.100   TCP   74 111 → 41990 [SYN, ACK] Seq=0 Ack
37 0.095511261   192.168.50.100   192.168.50.101   TCP   66 41990 → 111 [ACK] Seq=1 Ack=1 Wi
38 0.095649694   192.168.50.100   192.168.50.101   TCP   74 44228 → 445 [SYN] Seq=0 Win=6424
39 0.095668541   192.168.50.101   192.168.50.100   TCP   60 199 → 42660 [RST, ACK] Seq=1 Ack
40 0.095781664   192.168.50.100   192.168.50.101   TCP   74 55480 → 23 [SYN] Seq=0 Win=64240
41 0.095962483   192.168.50.100   192.168.50.101   TCP   66 34218 → 80 [RST, ACK] Seq=1 Ack=
42 0.095972560   192.168.50.101   192.168.50.100   TCP   74 445 → 44228 [SYN, ACK] Seq=0 Ack
43 0.096077623   192.168.50.100   192.168.50.101   TCP   66 44228 → 445 [ACK] Seq=1 Ack=1 Wi
44 0.096134313   192.168.50.101   192.168.50.100   TCP   74 23 → 55480 [SYN, ACK] Seq=0 Ack=
```

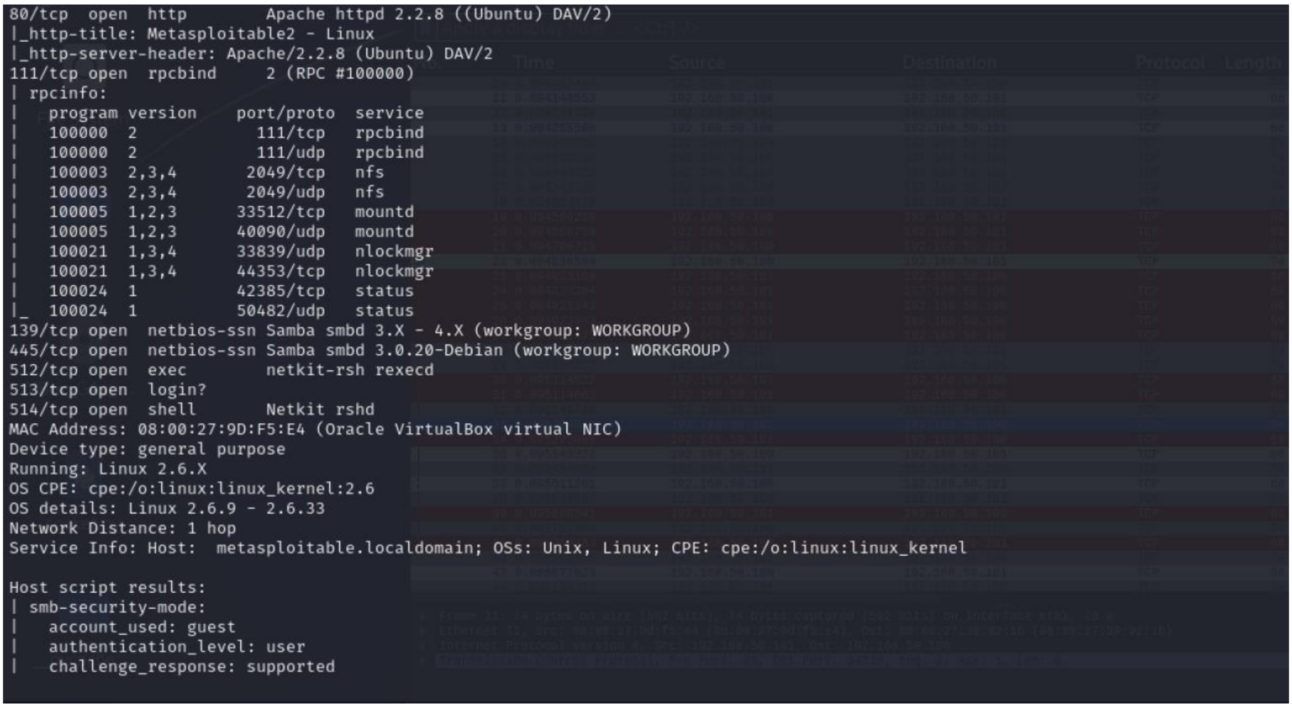
Netcat -A



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org )
at 2024-01-07 06:40 EST
Nmap scan report for 192.168.50.101
Host is up (0.00074s 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)
```



```
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:9D:F5:E4 (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:
| smb-security-mode:
|   account_used: guest
|   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: 2024-01-07T06:41:30-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h30m01s, deviation: 3h32m08s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   0.74 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 76.51 seconds

┌──(kali㉿kali)-[~]
└─$ █
```



```
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      33512/tcp   mountd
|   100005  1,2,3      40090/udp   mountd
|   100021  1,3,4      33839/udp   nlockmgr
|   100021  1,3,4      44353/tcp   nlockmgr
|   100024  1          42385/tcp   status
|_  100024  1          50482/udp   status
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: 08:00:27:9D:F5:E4 (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:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```