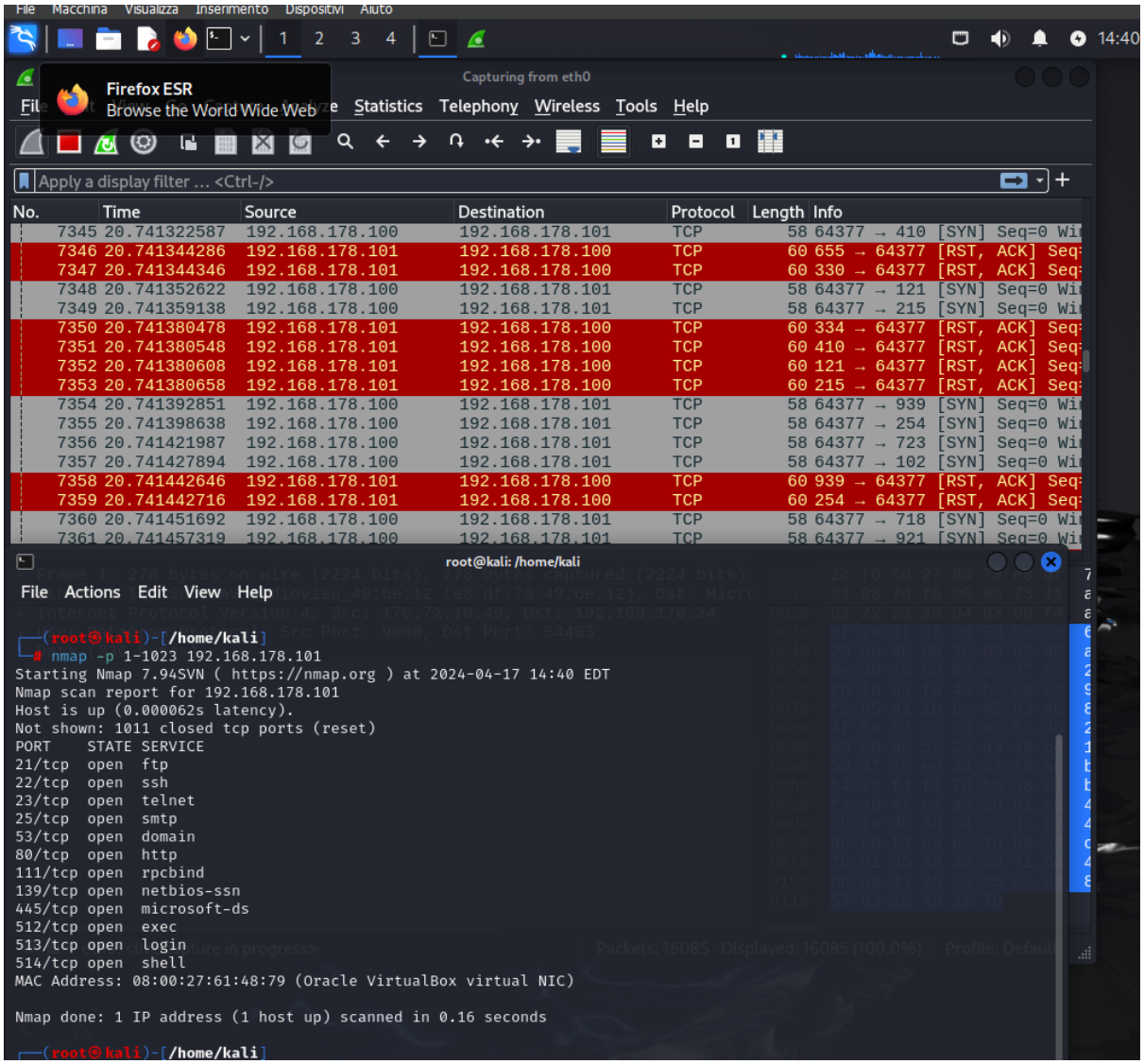
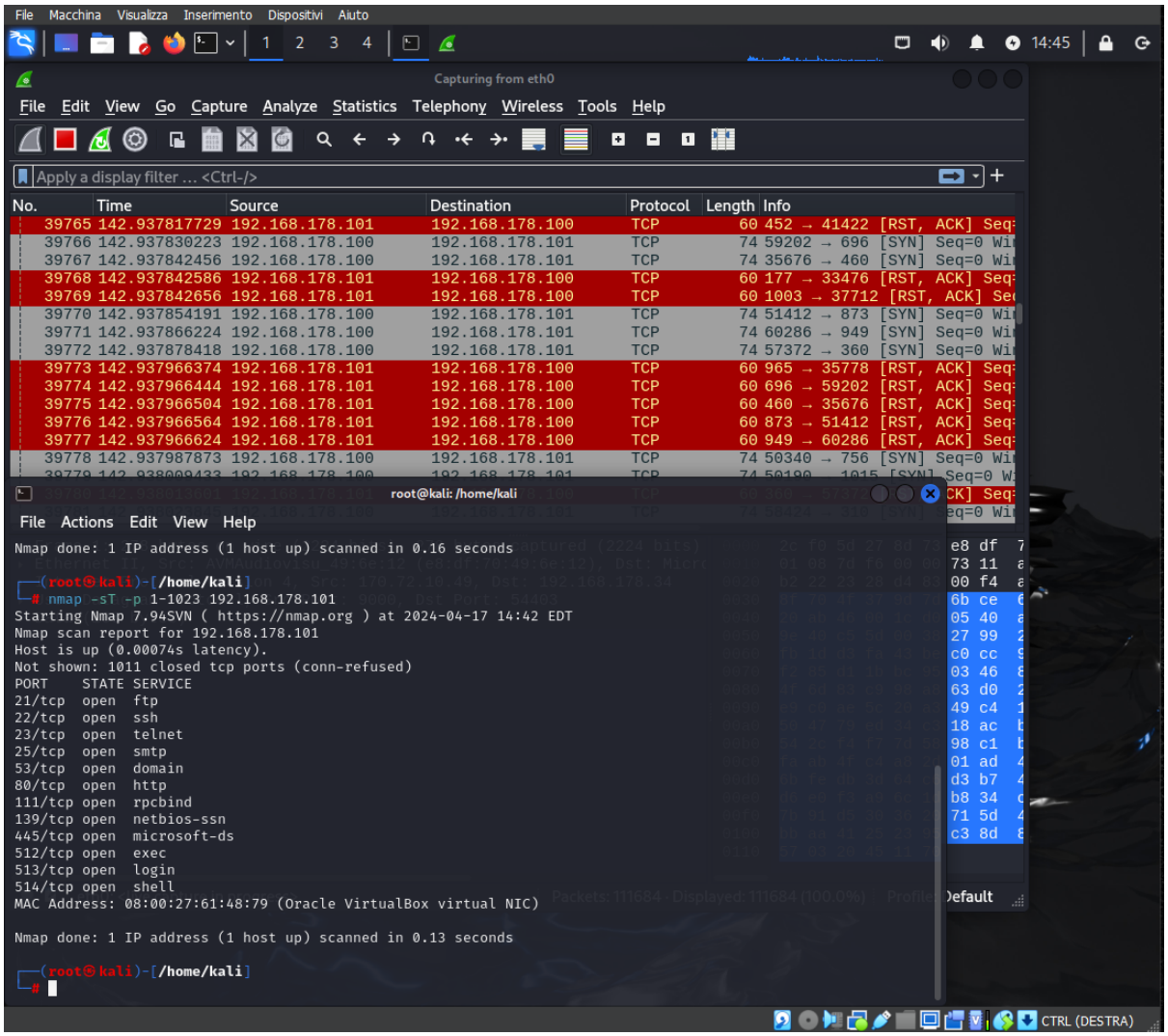
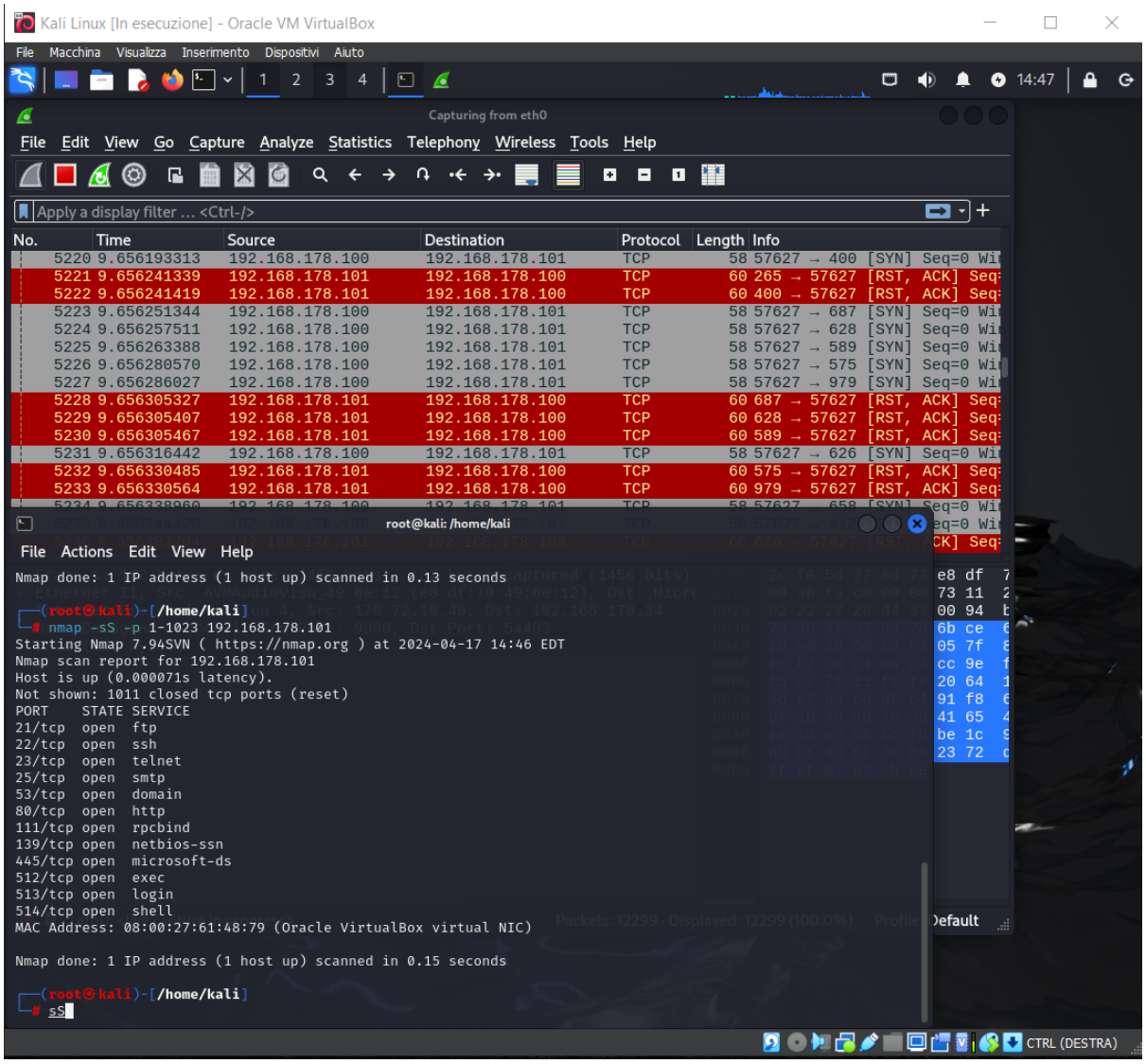
Scan TCP


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
14:40
Firefox ESR
Browse the World Wide Web
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7345 20.741322587 192.168.178.100 192.168.178.101 TCP 58 64377 → 410 [SYN] Seq=0 Wi
7346 20.741344286 192.168.178.101 192.168.178.100 TCP 60 655 → 64377 [RST, ACK] Seq
7347 20.741344346 192.168.178.101 192.168.178.100 TCP 60 330 → 64377 [RST, ACK] Seq
7348 20.741352622 192.168.178.100 192.168.178.101 TCP 58 64377 → 121 [SYN] Seq=0 Wi
7349 20.741359138 192.168.178.100 192.168.178.101 TCP 58 64377 → 215 [SYN] Seq=0 Wi
7350 20.741380478 192.168.178.101 192.168.178.100 TCP 60 334 → 64377 [RST, ACK] Seq
7351 20.741380548 192.168.178.101 192.168.178.100 TCP 60 410 → 64377 [RST, ACK] Seq
7352 20.741380608 192.168.178.101 192.168.178.100 TCP 60 121 → 64377 [RST, ACK] Seq
7353 20.741380658 192.168.178.101 192.168.178.100 TCP 60 215 → 64377 [RST, ACK] Seq
7354 20.741392851 192.168.178.100 192.168.178.101 TCP 58 64377 → 939 [SYN] Seq=0 Wi
7355 20.741398638 192.168.178.100 192.168.178.101 TCP 58 64377 → 254 [SYN] Seq=0 Wi
7356 20.741421987 192.168.178.100 192.168.178.101 TCP 58 64377 → 723 [SYN] Seq=0 Wi
7357 20.741427894 192.168.178.100 192.168.178.101 TCP 58 64377 → 102 [SYN] Seq=0 Wi
7358 20.741442646 192.168.178.101 192.168.178.100 TCP 60 939 → 64377 [RST, ACK] Seq
7359 20.741442716 192.168.178.101 192.168.178.100 TCP 60 254 → 64377 [RST, ACK] Seq
7360 20.741451692 192.168.178.100 192.168.178.101 TCP 58 64377 → 718 [SYN] Seq=0 Wi
7361 20.741457319 192.168.178.100 192.168.178.101 TCP 58 64377 → 921 [SYN] Seq=0 Wi
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1-1023 192.168.178.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-17 14:40 EDT
Nmap scan report for 192.168.178.101
Host is up (0.000062s latency).
Not shown: 1011 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: 08:00:27:61:48:79 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
┌──(root㉿kali)-[/home/kali]

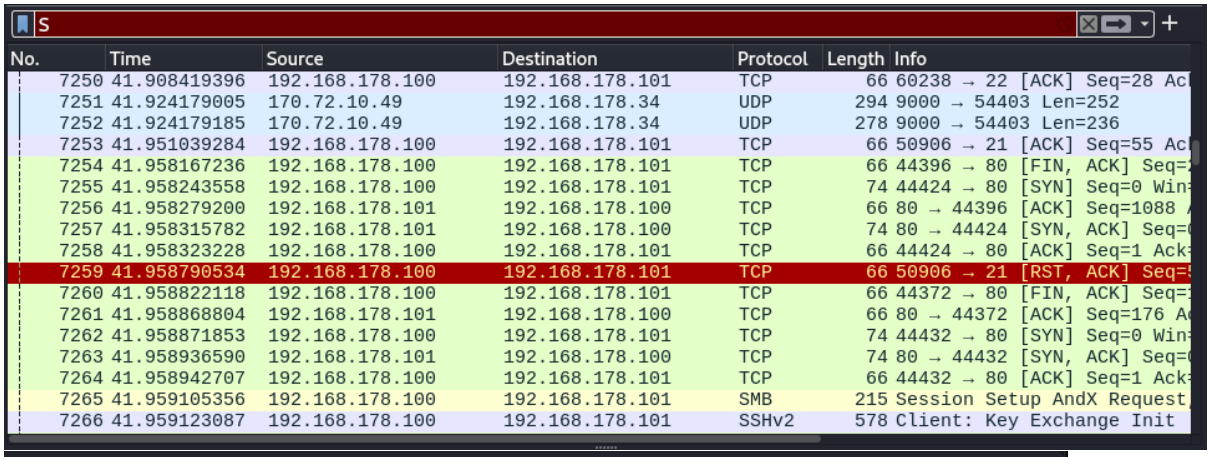
Scan TCP –sT più aggressivo, spam di syn-ack, molto “rumoroso”, spam di pacchetti molto più grande rispetto all’opzione -sS



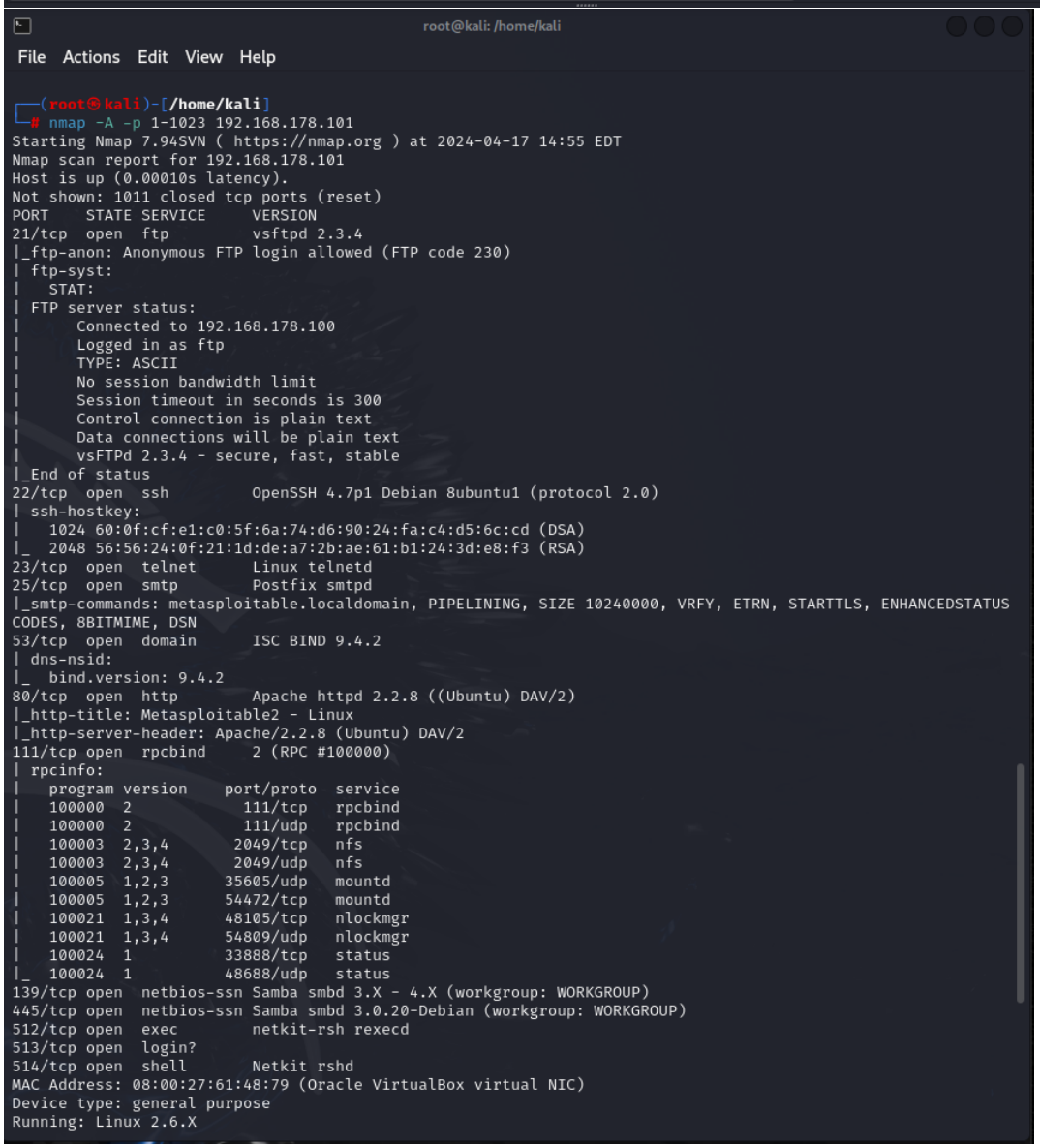
Scan SYN –sS più “silenzioso”, non conclude il three-way handshake



Risultati dell’opzione -A su scan TCP



No.	Time	Source	Destination	Protocol	Length	Info
7250	41.908419396	192.168.178.100	192.168.178.101	TCP	66	60238 → 22 [ACK] Seq=28 Ac
7251	41.924179005	170.72.10.49	192.168.178.34	UDP	294	9000 → 54403 Len=252
7252	41.924179185	170.72.10.49	192.168.178.34	UDP	278	9000 → 54403 Len=236
7253	41.951039284	192.168.178.100	192.168.178.101	TCP	66	50906 → 21 [ACK] Seq=55 Ac
7254	41.958167236	192.168.178.100	192.168.178.101	TCP	66	44396 → 80 [FIN, ACK] Seq=
7255	41.958243558	192.168.178.100	192.168.178.101	TCP	74	44424 → 80 [SYN] Seq=0 Win
7256	41.958279200	192.168.178.101	192.168.178.100	TCP	66	80 → 44396 [ACK] Seq=1088
7257	41.958315782	192.168.178.101	192.168.178.100	TCP	74	80 → 44424 [SYN, ACK] Seq=
7258	41.958323228	192.168.178.100	192.168.178.101	TCP	66	44424 → 80 [ACK] Seq=1 Ack
7259	41.958790534	192.168.178.100	192.168.178.101	TCP	66	50906 → 21 [RST, ACK] Seq=
7260	41.958822118	192.168.178.100	192.168.178.101	TCP	66	44372 → 80 [FIN, ACK] Seq=
7261	41.958868804	192.168.178.101	192.168.178.100	TCP	66	80 → 44372 [ACK] Seq=176 A
7262	41.958871853	192.168.178.100	192.168.178.101	TCP	74	44432 → 80 [SYN] Seq=0 Win
7263	41.958936590	192.168.178.101	192.168.178.100	TCP	74	80 → 44432 [SYN, ACK] Seq=
7264	41.958942707	192.168.178.100	192.168.178.101	TCP	66	44432 → 80 [ACK] Seq=1 Ack
7265	41.959105356	192.168.178.100	192.168.178.101	SMB	215	Session Setup AndX Request
7266	41.959123087	192.168.178.100	192.168.178.101	SSHv2	578	Client: Key Exchange Init



```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap -A -p 1-1023 192.168.178.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 14:55 EDT
Nmap scan report for 192.168.178.101
Host is up (0.00010s latency).
Not shown: 1011 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 192.168.178.100
|      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      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUS
CODES, 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      35605/udp   mountd
|   100005  1,2,3      54472/tcp   mountd
|   100021  1,3,4      48105/tcp   nlockmgr
|   100021  1,3,4      54809/udp   nlockmgr
|   100024  1          33888/tcp   status
|_  100024  1          48688/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: 08:00:27:61:48:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```