W10D4 Report

Una volta accertato l'indirizzo ip di metasploitable, partiamo con la scansione.

- nmap -sn -PE <target>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.1.101
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:27 CET
Nmap scan report for 192.168.1.101
Host is up (0.0065s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

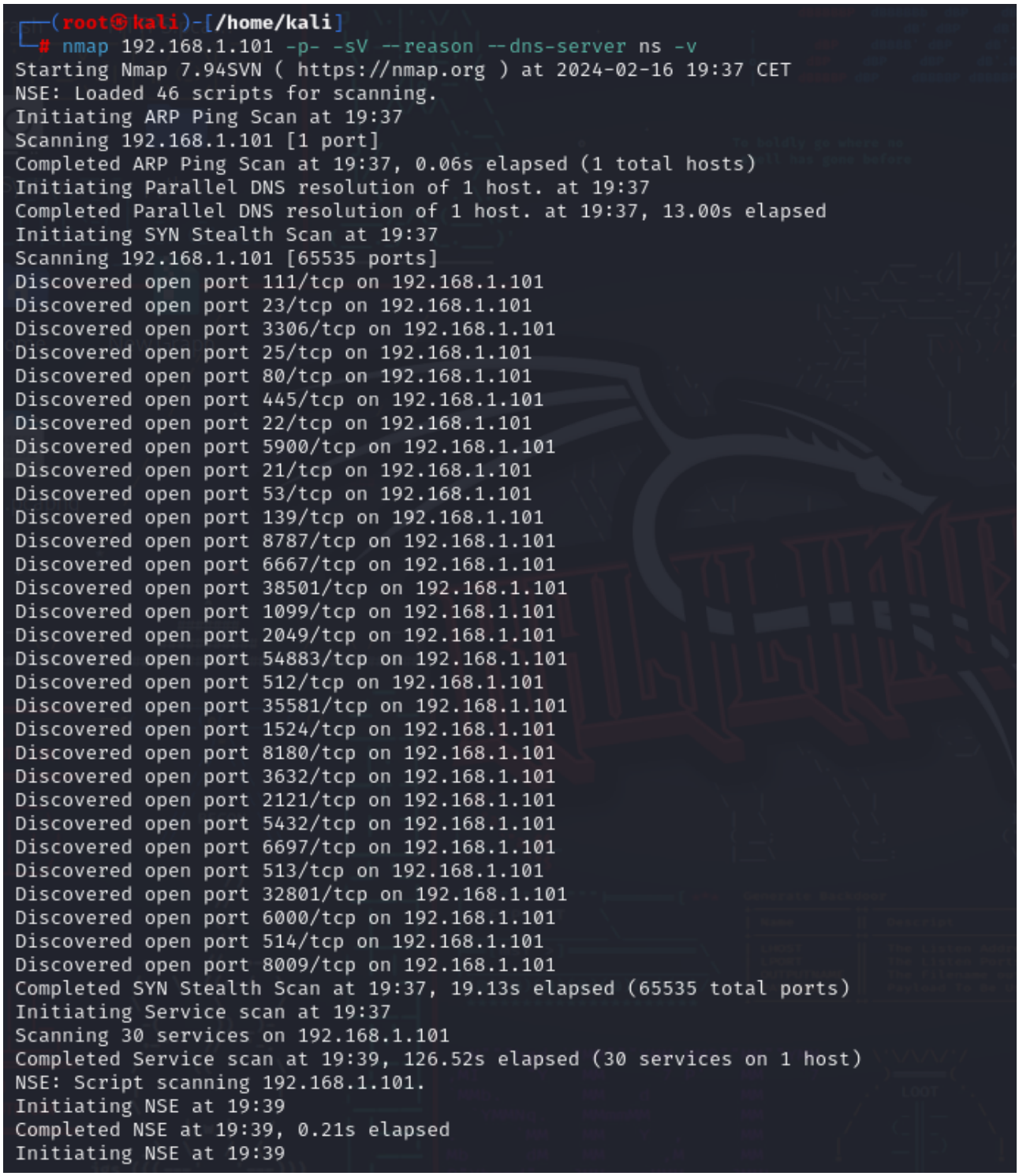
- netdiscover -r <target>

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 114 Captured ARP Req/Rep packets, from 12 hosts.   Total size: 6840
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 192.168.1.194   90:11:95:c0:01:c7      2     120  Amazon Technologies Inc.
 192.168.1.234   04:56:e5:79:08:0b      6     360  Intel Corporate
 192.168.1.1     a0:b5:3c:8b:f1:db     87    5220  Technicolor Delivery Technolog
 192.168.1.21    52:fc:80:80:7f:74      1      60  Unknown vendor
 192.168.1.16    74:df:bf:2d:aa:02      5     300  Liteon Technology Corporation
 192.168.1.101   08:00:27:44:05:c4      5     300  PCS Systemtechnik GmbH
 192.168.1.41    64:e7:d8:5a:c9:64      1      60  Samsung Electronics Co.,Ltd
 192.168.1.49    7c:16:89:7d:09:fc      1      60  Sagemcom Broadband SAS
 192.168.1.97    b0:f7:c4:aa:04:b7      1      60  Amazon Technologies Inc.
 192.168.1.191   14:c9:cf:b4:af:4c      1      60  Sigmastar Technology Ltd.
 192.168.1.193   0c:ec:84:14:fe:3b      3     180  Shenzhen TINNO Mobile Technolo
 192.168.1.198   fa:a2:d8:d8:3a:7d      1      60  Unknown vendor
```

- nmap <target> –top-ports 10 –open

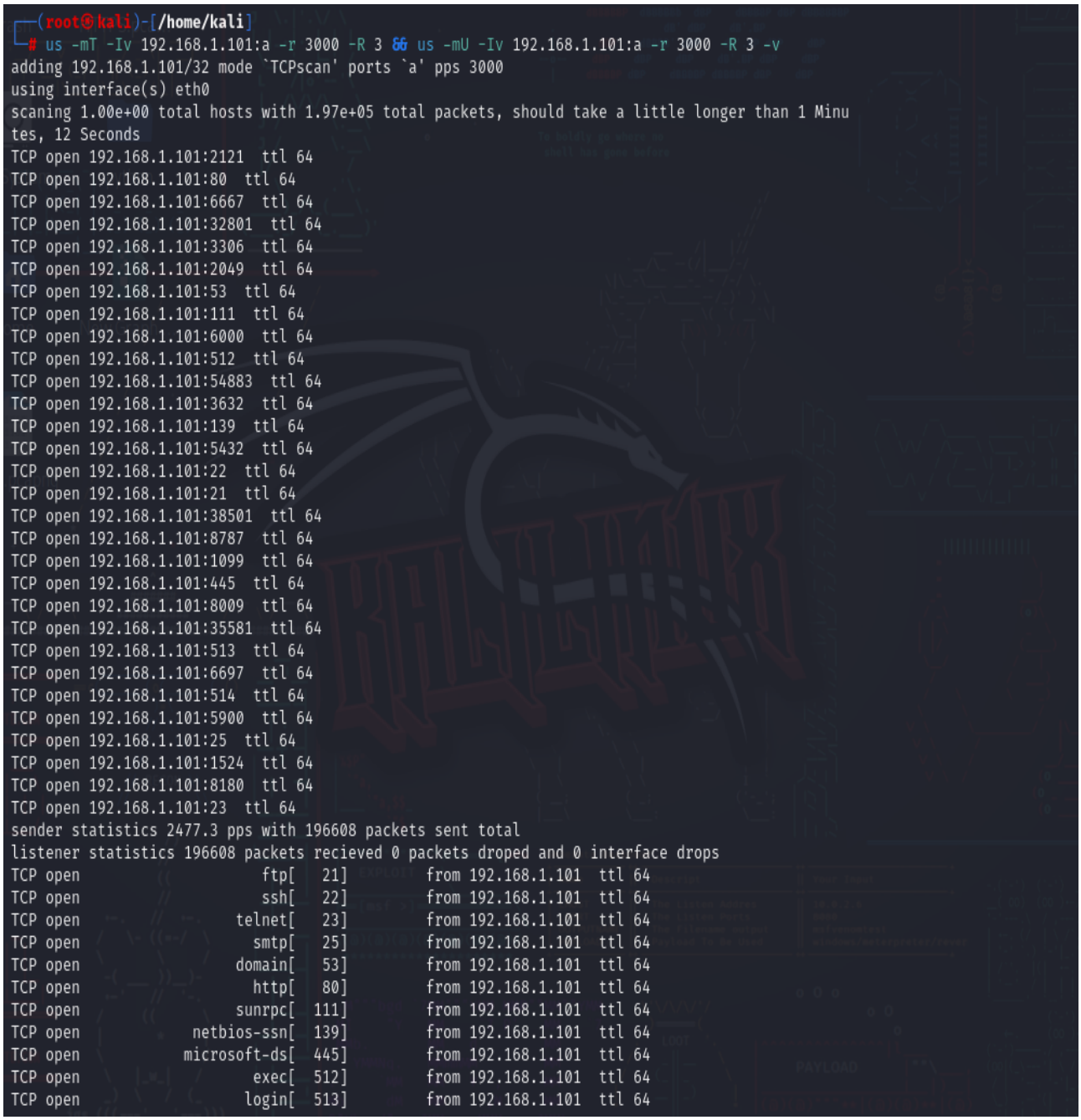
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.101 --top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:34 CET
Nmap scan report for 192.168.1.101
Host is up (0.011s latency).
Not shown: 3 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

- nmap <target> -p- -sV –reason –dns-server ns



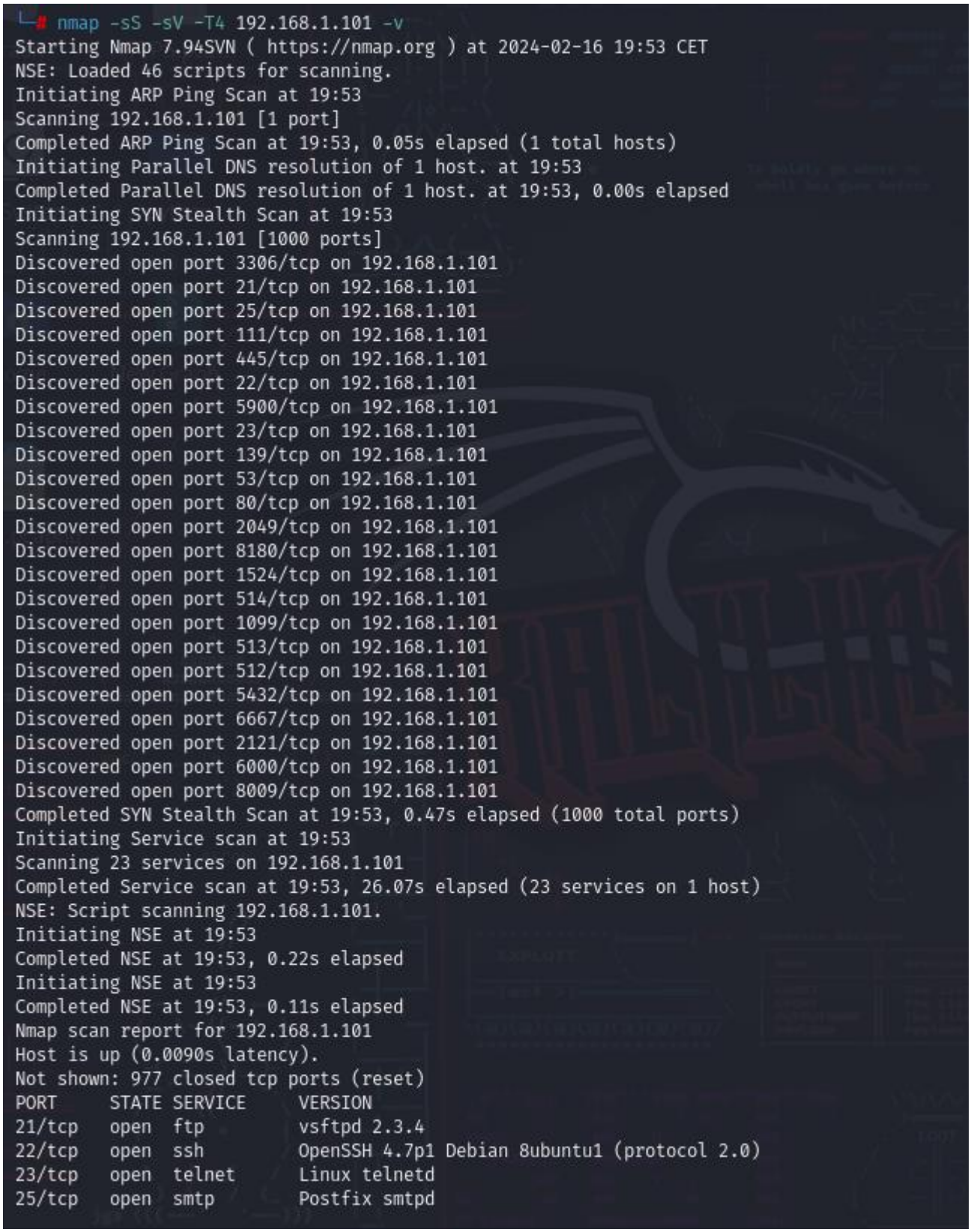
```
Completed NSE at 19:39, 0.17s elapsed
Nmap scan report for 192.168.1.101
Host is up, received arp-response (0.0017s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGR
OUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGR
OUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login       syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1
ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd (Admin email admin@Metasploi
table.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/r
uby/1.8/drb)
32801/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
35581/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
38501/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
54883/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.39 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
```

- us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv <target>:a -r 3000 -R 3



```
TCP open                 distcc[ 3632]         from 192.168.1.101  ttl 64
TCP open              postgresql[ 5432]         from 192.168.1.101  ttl 64
TCP open                 winvnc[ 5900]         from 192.168.1.101  ttl 64
TCP open                    x11[ 6000]         from 192.168.1.101  ttl 64
TCP open                    irc[ 6667]         from 192.168.1.101  ttl 64
TCP open                unknown[ 6697]         from 192.168.1.101  ttl 64
TCP open                unknown[ 8009]         from 192.168.1.101  ttl 64
TCP open                unknown[ 8180]         from 192.168.1.101  ttl 64
TCP open                msgsrvr[ 8787]         from 192.168.1.101  ttl 64
TCP open                unknown[32801]         from 192.168.1.101  ttl 64
TCP open                unknown[35581]         from 192.168.1.101  ttl 64
TCP open                unknown[38501]         from 192.168.1.101  ttl 64
TCP open                unknown[54883]         from 192.168.1.101  ttl 64
adding 192.168.1.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
added module payload for port 1900 proto 17
added module payload for port 53 proto 17
added module payload for port 80 proto 6
added module payload for port 518 proto 17
added module payload for port 80 proto 6
added module payload for port 5060 proto 17
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minu
tes, 12 Seconds
drone type Unknown on fd 4 is version 1.1
drone type Unknown on fd 3 is version 1.1
added module payload for port 1900 proto 17
added module payload for port 53 proto 17
added module payload for port 80 proto 6
added module payload for port 518 proto 17
added module payload for port 80 proto 6
added module payload for port 5060 proto 17
scan iteration 1 out of 1
using pcap filter: `dst 192.168.1.100 and ! src 192.168.1.100 and (udp)'
using TSC delay
UDP open 192.168.1.101:53  ttl 64
UDP open 192.168.1.101:111  ttl 64
UDP open 192.168.1.101:137  ttl 64
UDP open 192.168.1.101:44220  ttl 64
UDP open 192.168.1.101:2049  ttl 64
UDP open 192.168.1.101:46172  ttl 64
UDP open 192.168.1.101:51160  ttl 64
sender statistics 2720.1 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets droped and 0 interface drops
UDP open                 domain[   53]         from 192.168.1.101  ttl 64
UDP open                 sunrpc[  111]         from 192.168.1.101  ttl 64
UDP open             netbios-ns[  137]         from 192.168.1.101  ttl 64
UDP open                  shilp[ 2049]         from 192.168.1.101  ttl 64
UDP open                unknown[44220]         from 192.168.1.101  ttl 64
UDP open                unknown[46172]         from 192.168.1.101  ttl 64
UDP open                unknown[51160]         from 192.168.1.101  ttl 64
```

- nmap -sS -sV -T4 <target>



```
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)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: c
pe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.19 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

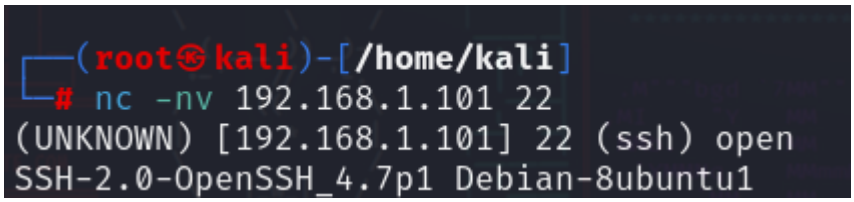
- hping3 –scan known <target>

```
┌──(root㉿kali)-[/home/kali]
└─# hping3 --scan known 192.168.1.101
Scanning 192.168.1.101 (192.168.1.101), port known
264 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (
139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ing
reslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 irc
d) (6697 ircs-u)
```

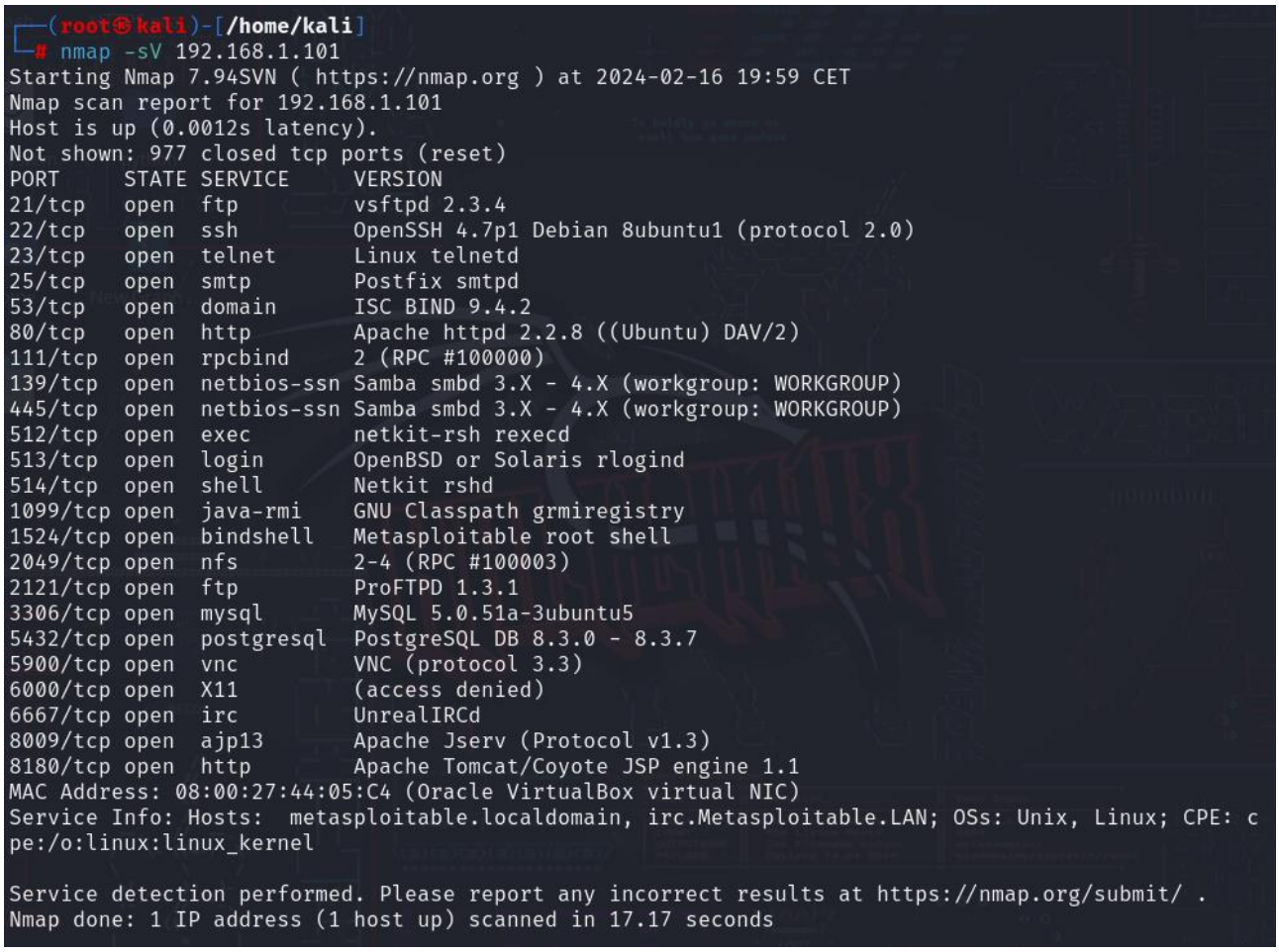
- nc -nvz <target> 1-1024

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvz 192.168.1.101 1-1024
(UNKNOWN) [192.168.1.101] 514 (shell) open
(UNKNOWN) [192.168.1.101] 513 (login) open
(UNKNOWN) [192.168.1.101] 512 (exec) open
(UNKNOWN) [192.168.1.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.101] 111 (sunrpc) open
(UNKNOWN) [192.168.1.101] 80 (http) open
(UNKNOWN) [192.168.1.101] 53 (domain) open
(UNKNOWN) [192.168.1.101] 25 (smtp) open
(UNKNOWN) [192.168.1.101] 23 (telnet) open
(UNKNOWN) [192.168.1.101] 22 (ssh) open
(UNKNOWN) [192.168.1.101] 21 (ftp) open
```

- nc -nv <target> 22



- nmap -sV <target>



- nmap -f –mtu=512 <target>