W10D4 - Pratica

```
┌──(root㉿kali)-[~]
└─# nmap -sn -PE 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 13:46 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0017s latency).
MAC Address: 08:00:27:3E:92:45 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.50.101
```

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

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.101  08:00:27:3e:92:45      1      60  PCS Systemtechnik GmbH
```

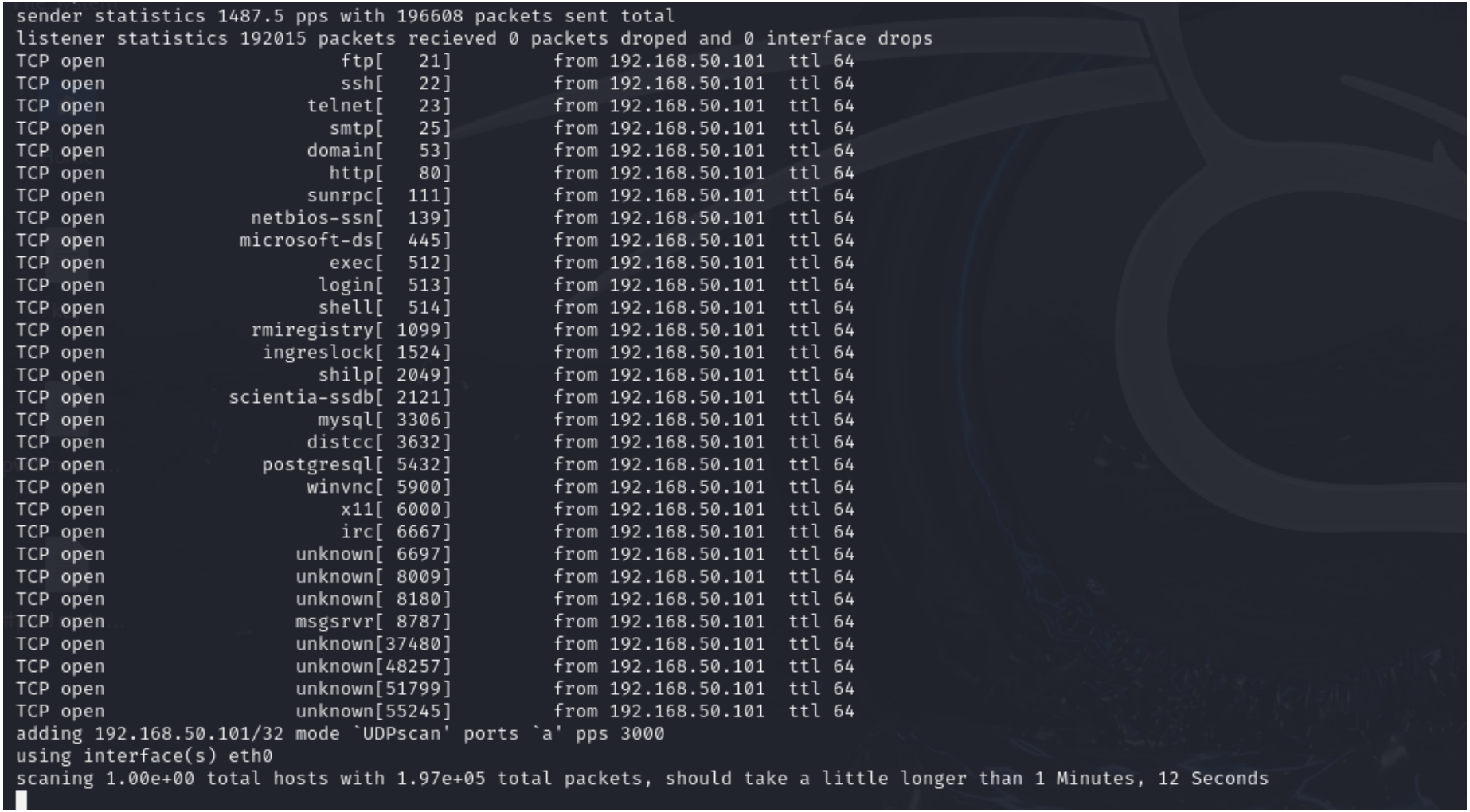
```
┌──(root㉿kali)-[~]
└─# crackmapexec ftp 192.168.50.101

[*] completed: 100.00% (1/1)
```

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 14:10 EDT
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.101 -p- -sV --reason --dns-server ns
```

```
┌──(root㉿kali)-[~]
└─# us -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3
adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:22  ttl 64
TCP open 192.168.50.101:445  ttl 64
TCP open 192.168.50.101:55245  ttl 64
TCP open 192.168.50.101:2121  ttl 64
TCP open 192.168.50.101:6000  ttl 64
TCP open 192.168.50.101:8180  ttl 64
TCP open 192.168.50.101:111  ttl 64
TCP open 192.168.50.101:53  ttl 64
TCP open 192.168.50.101:3632  ttl 64
TCP open 192.168.50.101:139  ttl 64
TCP open 192.168.50.101:8787  ttl 64
TCP open 192.168.50.101:37480  ttl 64
TCP open 192.168.50.101:25  ttl 64
TCP open 192.168.50.101:6697  ttl 64
TCP open 192.168.50.101:1524  ttl 64
TCP open 192.168.50.101:5432  ttl 64
TCP open 192.168.50.101:1099  ttl 64
TCP open 192.168.50.101:21  ttl 64
TCP open 192.168.50.101:6667  ttl 64
TCP open 192.168.50.101:3306  ttl 64
TCP open 192.168.50.101:514  ttl 64
TCP open 192.168.50.101:512  ttl 64
TCP open 192.168.50.101:80  ttl 64
TCP open 192.168.50.101:2049  ttl 64
TCP open 192.168.50.101:48257  ttl 64
TCP open 192.168.50.101:5900  ttl 64
TCP open 192.168.50.101:23  ttl 64
TCP open 192.168.50.101:8009  ttl 64
TCP open 192.168.50.101:51799  ttl 64
TCP open 192.168.50.101:513  ttl 64
sender statistics 1487.5 pps with 196608 packets sent total
listener statistics 192015 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.101  ttl 64
TCP open                     ssh[   22]         from 192.168.50.101  ttl 64
TCP open                  telnet[   23]         from 192.168.50.101  ttl 64
TCP open                    smtp[   25]         from 192.168.50.101  ttl 64
```


sender statistics 1487.5 pps with 196608 packets sent total
listener statistics 192015 packets recieved 0 packets droped and 0 interface drops
TCP open ftp[21] from 192.168.50.101 ttl 64
TCP open ssh[22] from 192.168.50.101 ttl 64
TCP open telnet[23] from 192.168.50.101 ttl 64
TCP open smtp[25] from 192.168.50.101 ttl 64
TCP open domain[53] from 192.168.50.101 ttl 64
TCP open http[80] from 192.168.50.101 ttl 64
TCP open sunrpc[111] from 192.168.50.101 ttl 64
TCP open netbios-ssn[139] from 192.168.50.101 ttl 64
TCP open microsoft-ds[445] from 192.168.50.101 ttl 64
TCP open exec[512] from 192.168.50.101 ttl 64
TCP open login[513] from 192.168.50.101 ttl 64
TCP open shell[514] from 192.168.50.101 ttl 64
TCP open rmiregistry[1099] from 192.168.50.101 ttl 64
TCP open ingreslock[1524] from 192.168.50.101 ttl 64
TCP open shilp[2049] from 192.168.50.101 ttl 64
TCP open scientia-ssdb[2121] from 192.168.50.101 ttl 64
TCP open mysql[3306] from 192.168.50.101 ttl 64
TCP open distcc[3632] from 192.168.50.101 ttl 64
TCP open postgresql[5432] from 192.168.50.101 ttl 64
TCP open winvnc[5900] from 192.168.50.101 ttl 64
TCP open x11[6000] from 192.168.50.101 ttl 64
TCP open irc[6667] from 192.168.50.101 ttl 64
TCP open unknown[6697] from 192.168.50.101 ttl 64
TCP open unknown[8009] from 192.168.50.101 ttl 64
TCP open unknown[8180] from 192.168.50.101 ttl 64
TCP open msgsrvr[8787] from 192.168.50.101 ttl 64
TCP open unknown[37480] from 192.168.50.101 ttl 64
TCP open unknown[48257] from 192.168.50.101 ttl 64
TCP open unknown[51799] from 192.168.50.101 ttl 64
TCP open unknown[55245] from 192.168.50.101 ttl 64
adding 192.168.50.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds

```
TCP open                     x11[ 6000]         from 192.168.50.101  ttl 64
TCP open                     irc[ 6667]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 6697]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8009]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8180]         from 192.168.50.101  ttl 64
TCP open                 msgsrvr[ 8787]         from 192.168.50.101  ttl 64
TCP open                 unknown[37480]         from 192.168.50.101  ttl 64
TCP open                 unknown[48257]         from 192.168.50.101  ttl 64
TCP open                 unknown[51799]         from 192.168.50.101  ttl 64
TCP open                 unknown[55245]         from 192.168.50.101  ttl 64
adding 192.168.50.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
UDP open 192.168.50.101:137  ttl 64
UDP open 192.168.50.101:2049  ttl 64
UDP open 192.168.50.101:111  ttl 64
UDP open 192.168.50.101:42086  ttl 64
UDP open 192.168.50.101:53  ttl 64
UDP open 192.168.50.101:33659  ttl 64
sender statistics 2330.1 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets droped and 0 interface drops
UDP open                  domain[   53]         from 192.168.50.101  ttl 64
UDP open                  sunrpc[  111]         from 192.168.50.101  ttl 64
UDP open              netbios-ns[  137]         from 192.168.50.101  ttl 64
UDP open                   shilp[ 2049]         from 192.168.50.101  ttl 64
UDP open                 unknown[33659]         from 192.168.50.101  ttl 64
UDP open                 unknown[42086]         from 192.168.50.101  ttl 64
```

```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 15:26 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dn
s-servers
Nmap scan report for 192.168.50.101
Host is up (0.00051s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:3E:92:45 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.48 seconds

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), 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 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6
000 x11) (6667 ircd) (6697 ircs-u)

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

```
┌──(root㉿kali)-[~]
└─# nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 15:35 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dn
s-servers
Nmap scan report for 192.168.50.101
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:3E:92:45 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.98 seconds
```


┌──(root㉿kali)-[~]
└─# nmap -f --mtu=512 192.168.50.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-12 15:39 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0080s latency).
Not shown: 977 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
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:3E:92:45 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds