

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

```
(root@kali)-[/home/kali]
# nmap 192.168.1.101 -p- -sV --reason --dns-server ns -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:37 CET
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 19:37
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 19:37, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:37
Completed Parallel DNS resolution of 1 host. at 19:37, 13.00s elapsed
Initiating SYN Stealth Scan at 19:37
Scanning 192.168.1.101 [65535 ports]
Discovered open port 111/tcp on 192.168.1.101
Discovered open port 23/tcp on 192.168.1.101
Discovered open port 3306/tcp on 192.168.1.101
Discovered open port 25/tcp on 192.168.1.101
Discovered open port 80/tcp on 192.168.1.101
Discovered open port 445/tcp on 192.168.1.101
Discovered open port 22/tcp on 192.168.1.101
Discovered open port 5900/tcp on 192.168.1.101
Discovered open port 21/tcp on 192.168.1.101
Discovered open port 53/tcp on 192.168.1.101
Discovered open port 139/tcp on 192.168.1.101
Discovered open port 8787/tcp on 192.168.1.101
Discovered open port 6667/tcp on 192.168.1.101
Discovered open port 38501/tcp on 192.168.1.101
Discovered open port 1099/tcp on 192.168.1.101
Discovered open port 2049/tcp on 192.168.1.101
Discovered open port 54883/tcp on 192.168.1.101
Discovered open port 512/tcp on 192.168.1.101
Discovered open port 35581/tcp on 192.168.1.101
Discovered open port 1524/tcp on 192.168.1.101
Discovered open port 8180/tcp on 192.168.1.101
Discovered open port 3632/tcp on 192.168.1.101
Discovered open port 2121/tcp on 192.168.1.101
Discovered open port 5432/tcp on 192.168.1.101
Discovered open port 6697/tcp on 192.168.1.101
Discovered open port 513/tcp on 192.168.1.101
Discovered open port 32801/tcp on 192.168.1.101
Discovered open port 6000/tcp on 192.168.1.101
Discovered open port 514/tcp on 192.168.1.101
Discovered open port 8009/tcp on 192.168.1.101
Completed SYN Stealth Scan at 19:37, 19.13s elapsed (65535 total ports)
Initiating Service scan at 19:37
Scanning 30 services on 192.168.1.101
Completed Service scan at 19:39, 126.52s elapsed (30 services on 1 host)
NSE: Script scanning 192.168.1.101.
Initiating NSE at 19:39
Completed NSE at 19:39, 0.21s elapsed
Initiating NSE at 19:39
```

```

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      TTL  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/drbr)
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 -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3`

```
(root@kali)-[/home/kali]
# us -mT -lv 192.168.1.101:a -r 3000 -R 3 && us -mU -lv 192.168.1.101:a -r 3000 -R 3 -v
adding 192.168.1.101/32 mode 'TCPscan' ports 'a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minute, 12 Seconds
TCP open 192.168.1.101:2121 ttl 64
TCP open 192.168.1.101:80 ttl 64
TCP open 192.168.1.101:6667 ttl 64
TCP open 192.168.1.101:32801 ttl 64
TCP open 192.168.1.101:3306 ttl 64
TCP open 192.168.1.101:2049 ttl 64
TCP open 192.168.1.101:53 ttl 64
TCP open 192.168.1.101:111 ttl 64
TCP open 192.168.1.101:6000 ttl 64
TCP open 192.168.1.101:512 ttl 64
TCP open 192.168.1.101:54883 ttl 64
TCP open 192.168.1.101:3632 ttl 64
TCP open 192.168.1.101:139 ttl 64
TCP open 192.168.1.101:5432 ttl 64
TCP open 192.168.1.101:22 ttl 64
TCP open 192.168.1.101:21 ttl 64
TCP open 192.168.1.101:38501 ttl 64
TCP open 192.168.1.101:8787 ttl 64
TCP open 192.168.1.101:1099 ttl 64
TCP open 192.168.1.101:445 ttl 64
TCP open 192.168.1.101:8009 ttl 64
TCP open 192.168.1.101:35581 ttl 64
TCP open 192.168.1.101:513 ttl 64
TCP open 192.168.1.101:6697 ttl 64
TCP open 192.168.1.101:514 ttl 64
TCP open 192.168.1.101:5900 ttl 64
TCP open 192.168.1.101:25 ttl 64
TCP open 192.168.1.101:1524 ttl 64
TCP open 192.168.1.101:8180 ttl 64
TCP open 192.168.1.101:23 ttl 64
sender statistics 2477.3 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets dropped and 0 interface drops
TCP open ftp[ 21] from 192.168.1.101 ttl 64
TCP open ssh[ 22] from 192.168.1.101 ttl 64
TCP open telnet[ 23] from 192.168.1.101 ttl 64
TCP open smtp[ 25] from 192.168.1.101 ttl 64
TCP open domain[ 53] from 192.168.1.101 ttl 64
TCP open http[ 80] from 192.168.1.101 ttl 64
TCP open sunrpc[ 111] from 192.168.1.101 ttl 64
TCP open netbios-ssn[ 139] from 192.168.1.101 ttl 64
TCP open microsoft-ds[ 445] from 192.168.1.101 ttl 64
TCP open exec[ 512] from 192.168.1.101 ttl 64
TCP open login[ 513] from 192.168.1.101 ttl 64
```

```
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      python 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
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minute, 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 dropped 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>`

```
nmap -sS -sV -T4 192.168.1.101 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:53 CET
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 19:53
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 19:53, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:53
Completed Parallel DNS resolution of 1 host. at 19:53, 0.00s elapsed
Initiating SYN Stealth Scan at 19:53
Scanning 192.168.1.101 [1000 ports]
Discovered open port 3306/tcp on 192.168.1.101
Discovered open port 21/tcp on 192.168.1.101
Discovered open port 25/tcp on 192.168.1.101
Discovered open port 111/tcp on 192.168.1.101
Discovered open port 445/tcp on 192.168.1.101
Discovered open port 22/tcp on 192.168.1.101
Discovered open port 5900/tcp on 192.168.1.101
Discovered open port 23/tcp on 192.168.1.101
Discovered open port 139/tcp on 192.168.1.101
Discovered open port 53/tcp on 192.168.1.101
Discovered open port 80/tcp on 192.168.1.101
Discovered open port 2049/tcp on 192.168.1.101
Discovered open port 8180/tcp on 192.168.1.101
Discovered open port 1524/tcp on 192.168.1.101
Discovered open port 514/tcp on 192.168.1.101
Discovered open port 1099/tcp on 192.168.1.101
Discovered open port 513/tcp on 192.168.1.101
Discovered open port 512/tcp on 192.168.1.101
Discovered open port 5432/tcp on 192.168.1.101
Discovered open port 6667/tcp on 192.168.1.101
Discovered open port 2121/tcp on 192.168.1.101
Discovered open port 6000/tcp on 192.168.1.101
Discovered open port 8009/tcp on 192.168.1.101
Completed SYN Stealth Scan at 19:53, 0.47s elapsed (1000 total ports)
Initiating Service scan at 19:53
Scanning 23 services on 192.168.1.101
Completed Service scan at 19:53, 26.07s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.1.101.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.22s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.11s elapsed
Nmap scan report for 192.168.1.101
Host is up (0.0090s 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
```



```

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        Netkit rshd
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: cpe:/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

```
(root@kali)-[/home/kali]
# nc -nv 192.168.1.101 22
(UNKNOWN) [192.168.1.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

- nmap -sV <target>

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 19:59 CET
Nmap scan report for 192.168.1.101
Host is up (0.0012s 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        OpenBSD or Solaris rlogind
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: 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 17.17 seconds
```


- `nmap -f -mtu=512 <target>`

```
(root@kali)-[/home/kali]
# nmap -f --mtu=512 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 20:02 CET
Nmap scan report for 192.168.1.101
Host is up (0.013s 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: 08:00:27:44:05:C4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```