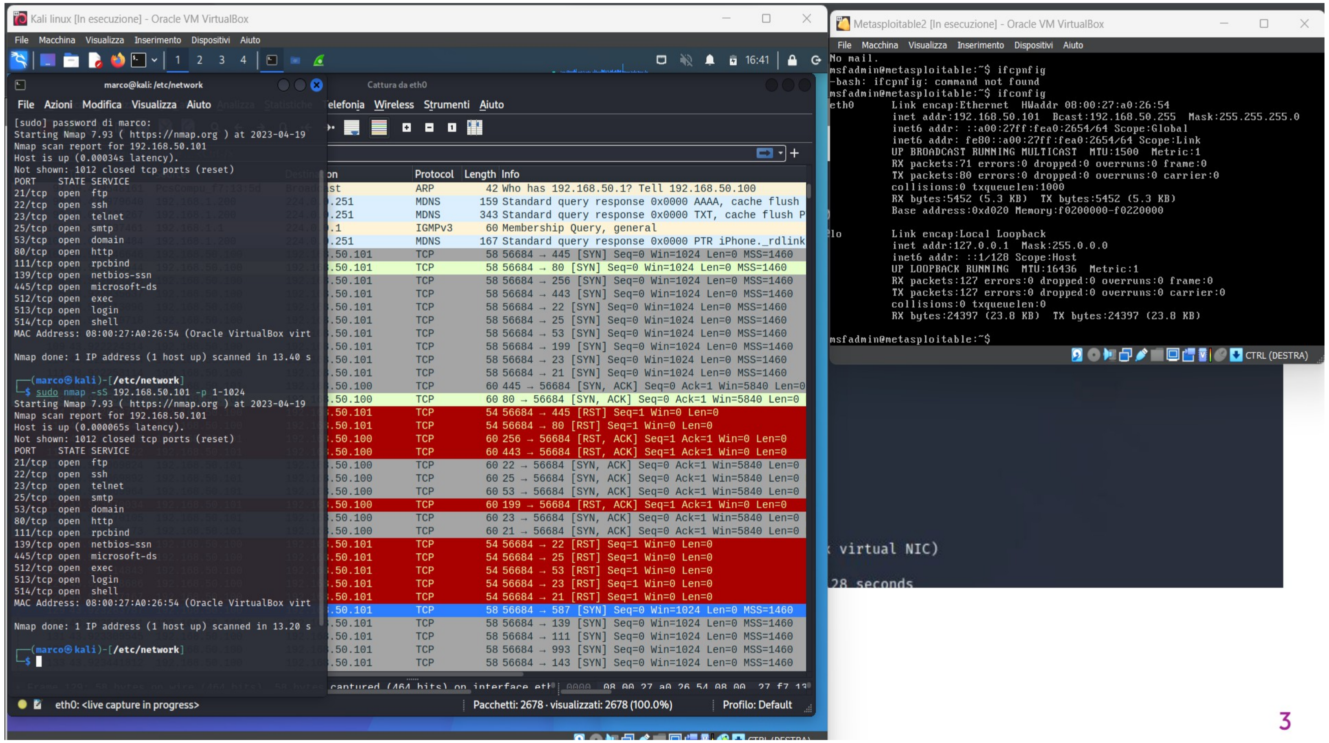
SCANSIONE NMAP -sS Syn Scan

FONTE – Kali Linux	TARGET – Metasplotable2	PORTE	STATO	SERVICE
192.168.50.100	192.168.50.101	21/tcp	open	ftp
192.168.50.100	192.168.50.101	22/tcp	open	ssh
192.168.50.100	192.168.50.101	23/tcp	open	telnet
192.168.50.100	192.168.50.101	25/tcp	open	smtp
192.168.50.100	192.168.50.101	53/tcp	open	domain
192.168.50.100	192.168.50.101	80/tcp	open	http
192.168.50.100	192.168.50.101	111/tcp	open	rpcbind
192.168.50.100	192.168.50.101	139/tcp	open	netbios-ssn
192.168.50.100	192.168.50.101	445/tcp	open	microsoft-ds
192.168.50.100	192.168.50.101	512/tcp	open	exec
192.168.50.100	192.168.50.101	513/tcp	open	login
192.168.50.100	192.168.50.101	514/tcp	open	shell

porte chiuse 1012

MAC Address: 08:00:27:A0:26:54 (Oracle VirtualBox virtual NIC)

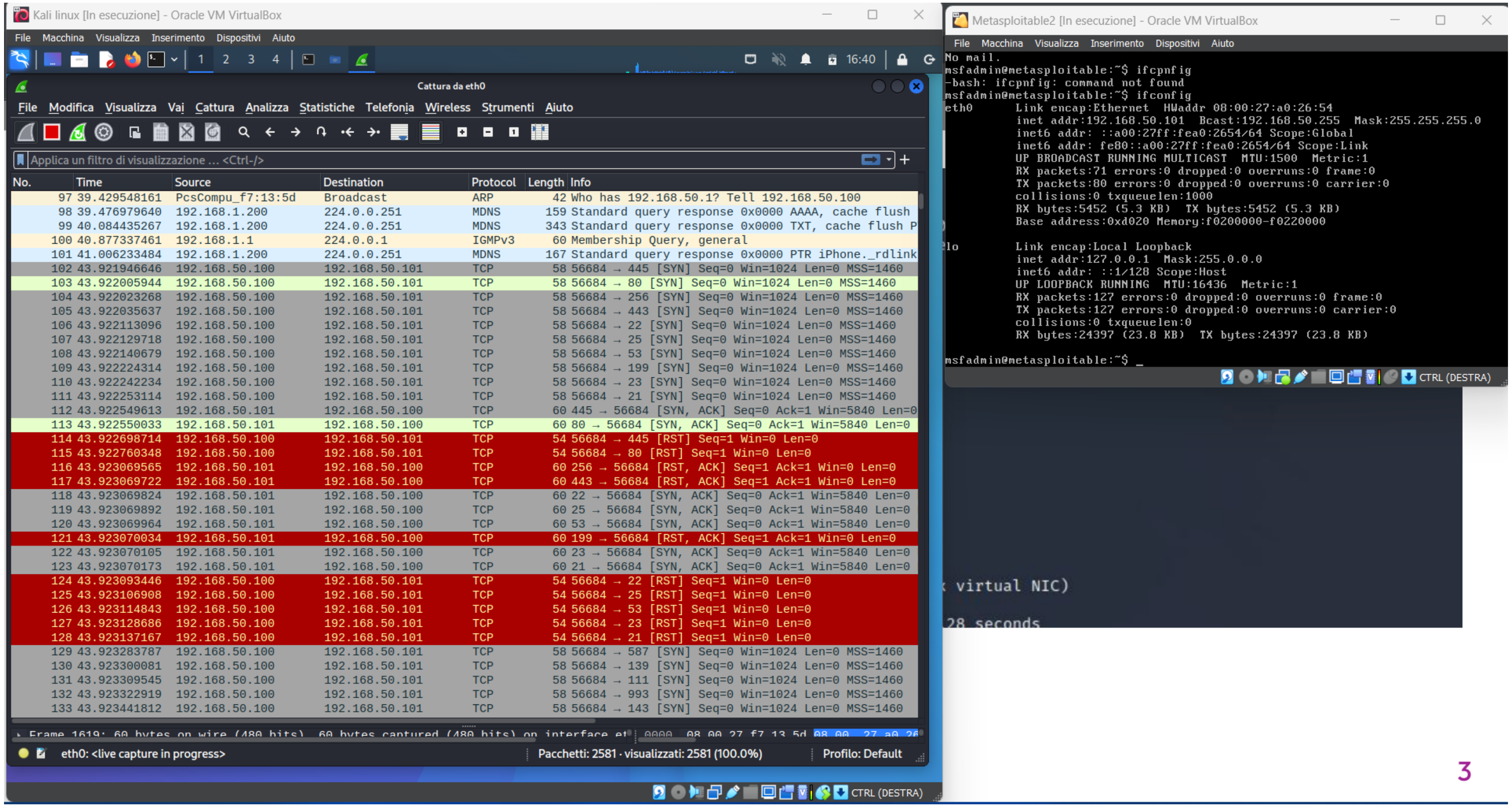

Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:41
marco@kali: /etc/network
File Azioni Modifica Visualizza Aiuto
Cattura da eth0
Telefonia Wireless Strumenti Aiuto
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)
virtual NIC)
28 seconds

```
[sudo] password di marco:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19
Nmap scan report for 192.168.50.101
Host is up (0.00034s 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
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:A0:26:54 (Oracle VirtualBox virt

Nmap done: 1 IP address (1 host up) scanned in 13.40 s

┌──(marco㉿kali)-[/etc/network]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19
Nmap scan report for 192.168.50.101
Host is up (0.000065s 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
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:A0:26:54 (Oracle VirtualBox virt

Nmap done: 1 IP address (1 host up) scanned in 13.20 s

┌──(marco㉿kali)-[/etc/network]
└─$ 
```

```
on          Protocol Length Info
st          ARP       42 Who has 192.168.50.1? Tell 192.168.50.100
.251        MDNS     159 Standard query response 0x0000 AAAA, cache flush
.251        MDNS     343 Standard query response 0x0000 TXT, cache flush P
.1          IGMPv3    60 Membership Query, general
.251        MDNS     167 Standard query response 0x0000 PTR iPhone._rdlink
.50.101     TCP       58 56684 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.100     TCP       60 445 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.100     TCP       60 80 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.101     TCP       54 56684 → 445 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       54 56684 → 80 [RST] Seq=1 Win=0 Len=0
.50.100     TCP       60 256 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100     TCP       60 443 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100     TCP       60 22 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.100     TCP       60 25 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.100     TCP       60 53 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.100     TCP       60 199 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100     TCP       60 23 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.100     TCP       60 21 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
.50.101     TCP       54 56684 → 22 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       54 56684 → 25 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       54 56684 → 53 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       54 56684 → 23 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       54 56684 → 21 [RST] Seq=1 Win=0 Len=0
.50.101     TCP       58 56684 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
.50.101     TCP       58 56684 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
captured (464 bits) on interface eth   0000  08 00 27 a0 26 54 08 00  27 f7 13
eth0: <live capture in progress>   Pacchetti: 2678 · visualizzati: 2678 (100.0%)   Profilo: Default
```

```
No mail.
msfadmin@metasploitable:~$ ifcpnfig
-bash: ifcpnfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:26:54
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: ::a00:27ff:fea0:2654/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea0:2654/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5452 (5.3 KB)  TX bytes:5452 (5.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24397 (23.8 KB)  TX bytes:24397 (23.8 KB)

msfadmin@metasploitable:~$
```

3


Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:40
Cattura da eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione … <Ctrl-/>
CTRL (DESTRA)
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)
virtual NIC)
28 seconds
3

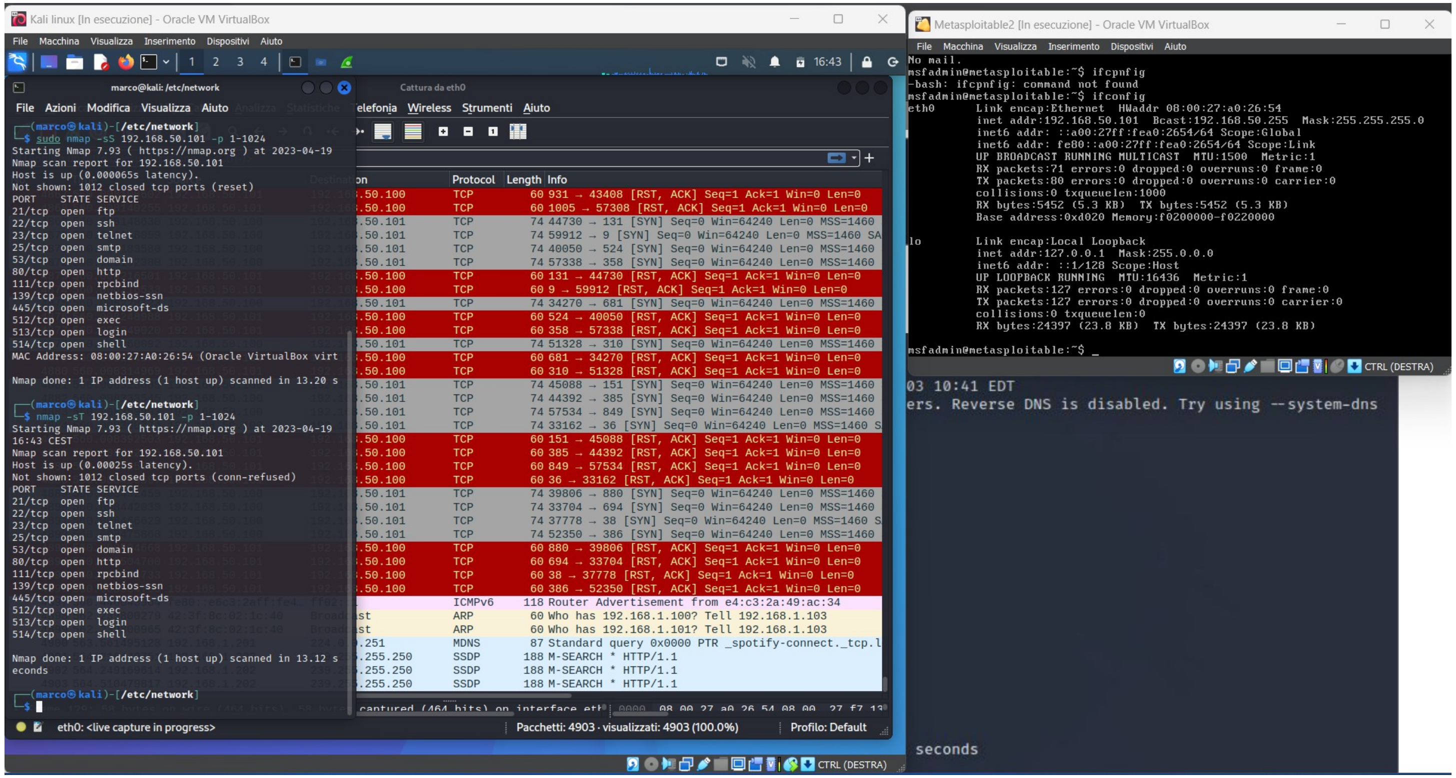
```
No.   Time           Source             Destination      Protocol  Length Info
   97 39.429548161   PcsCompu_f7:13:5d  Broadcast        ARP         42 Who has 192.168.50.1? Tell 192.168.50.100
   98 39.476979640   192.168.1.200      224.0.0.251      MDNS       159 Standard query response 0x0000 AAAA, cache flush
   99 40.084435267   192.168.1.200      224.0.0.251      MDNS       343 Standard query response 0x0000 TXT, cache flush P
  100 40.877337461   192.168.1.1        224.0.0.1        IGMPv3      60 Membership Query, general
  101 41.006233484   192.168.1.200      224.0.0.251      MDNS       167 Standard query response 0x0000 PTR iPhone._rdlink
  102 43.921946646   192.168.50.100     192.168.50.101   TCP         58 56684 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  103 43.922005944   192.168.50.100     192.168.50.101   TCP         58 56684 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  104 43.922023268   192.168.50.100     192.168.50.101   TCP         58 56684 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  105 43.922035637   192.168.50.100     192.168.50.101   TCP         58 56684 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  106 43.922113096   192.168.50.100     192.168.50.101   TCP         58 56684 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  107 43.922129718   192.168.50.100     192.168.50.101   TCP         58 56684 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  108 43.922140679   192.168.50.100     192.168.50.101   TCP         58 56684 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  109 43.922224314   192.168.50.100     192.168.50.101   TCP         58 56684 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  110 43.922242234   192.168.50.100     192.168.50.101   TCP         58 56684 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  111 43.922253114   192.168.50.100     192.168.50.101   TCP         58 56684 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  112 43.922549613   192.168.50.101     192.168.50.100   TCP         60 445 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  113 43.922550033   192.168.50.101     192.168.50.100   TCP         60 80 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  114 43.922698714   192.168.50.100     192.168.50.101   TCP         54 56684 → 445 [RST] Seq=1 Win=0 Len=0
  115 43.922760348   192.168.50.100     192.168.50.101   TCP         54 56684 → 80 [RST] Seq=1 Win=0 Len=0
  116 43.923069565   192.168.50.101     192.168.50.100   TCP         60 256 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  117 43.923069722   192.168.50.101     192.168.50.100   TCP         60 443 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  118 43.923069824   192.168.50.101     192.168.50.100   TCP         60 22 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  119 43.923069892   192.168.50.101     192.168.50.100   TCP         60 25 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  120 43.923069964   192.168.50.101     192.168.50.100   TCP         60 53 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  121 43.923070034   192.168.50.101     192.168.50.100   TCP         60 199 → 56684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  122 43.923070105   192.168.50.101     192.168.50.100   TCP         60 23 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  123 43.923070173   192.168.50.101     192.168.50.100   TCP         60 21 → 56684 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
  124 43.923093446   192.168.50.100     192.168.50.101   TCP         54 56684 → 22 [RST] Seq=1 Win=0 Len=0
  125 43.923106908   192.168.50.100     192.168.50.101   TCP         54 56684 → 25 [RST] Seq=1 Win=0 Len=0
  126 43.923114843   192.168.50.100     192.168.50.101   TCP         54 56684 → 53 [RST] Seq=1 Win=0 Len=0
  127 43.923128686   192.168.50.100     192.168.50.101   TCP         54 56684 → 23 [RST] Seq=1 Win=0 Len=0
  128 43.923137167   192.168.50.100     192.168.50.101   TCP         54 56684 → 21 [RST] Seq=1 Win=0 Len=0
  129 43.923283787   192.168.50.100     192.168.50.101   TCP         58 56684 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  130 43.923300081   192.168.50.100     192.168.50.101   TCP         58 56684 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  131 43.923309545   192.168.50.100     192.168.50.101   TCP         58 56684 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  132 43.923322919   192.168.50.100     192.168.50.101   TCP         58 56684 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  133 43.923441812   192.168.50.100     192.168.50.101   TCP         58 56684 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

› Frame 1619: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface et   0000  08 00 27 f7 13 5d 08 00 27 a0 26

eth0: <live capture in progress>     Pacchetti: 2581 · visualizzati: 2581 (100.0%)     Profilo: Default
```

```
No mail.
msfadmin@metasploitable:~$ ifcpnfig
-bash: ifcpnfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:26:54
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: ::a00:27ff:fea0:2654/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea0:2654/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5452 (5.3 KB)  TX bytes:5452 (5.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24397 (23.8 KB)  TX bytes:24397 (23.8 KB)

msfadmin@metasploitable:~$ _
```

SCANSIONE NMAP -sT tcp Scan

FONTE – Kali Linux	TARGET – Metasplotable2	PORTE	STATO	SERVICE
192.168.50.100	192.168.50.101	21/tcp	open	ftp
192.168.50.100	192.168.50.101	22/tcp	open	ssh
192.168.50.100	192.168.50.101	23/tcp	open	telnet
192.168.50.100	192.168.50.101	25/tcp	open	smtp
192.168.50.100	192.168.50.101	53/tcp	open	domain
192.168.50.100	192.168.50.101	80/tcp	open	http
192.168.50.100	192.168.50.101	111/tcp	open	rpcbind
192.168.50.100	192.168.50.101	139/tcp	open	netbios-ssn
192.168.50.100	192.168.50.101	445/tcp	open	microsoft-ds
192.168.50.100	192.168.50.101	512/tcp	open	exec
192.168.50.100	192.168.50.101	513/tcp	open	login
192.168.50.100	192.168.50.101	514/tcp	open	shell

porte chiuse 1012

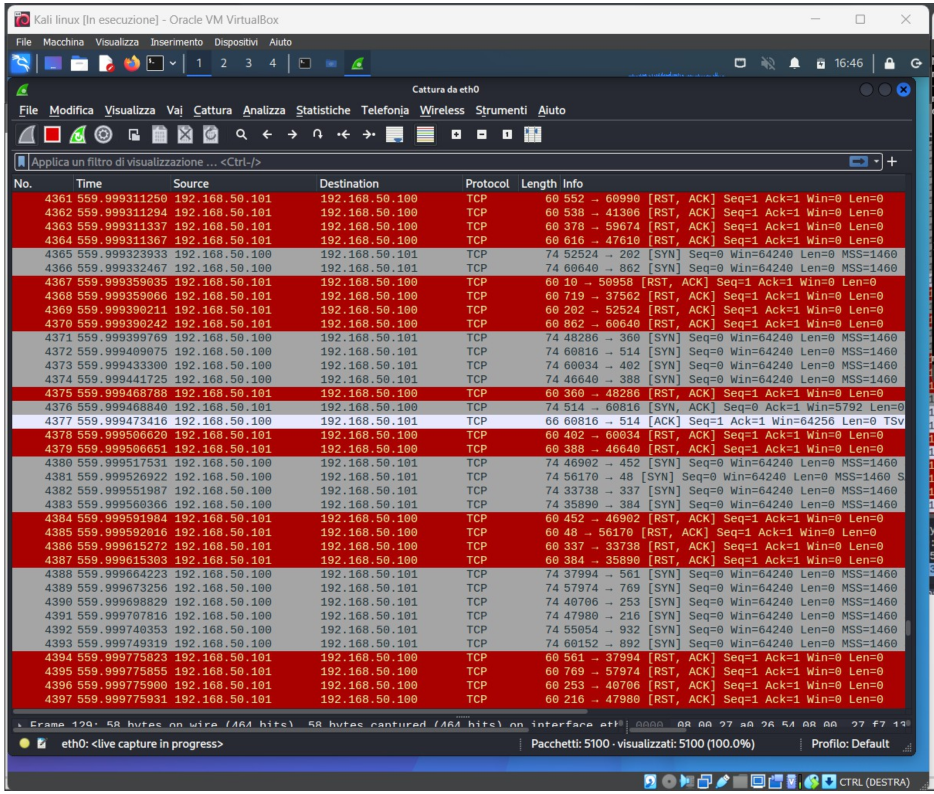

Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:43
marco@kali: /etc/network
File Azioni Modifica Visualizza Aiuto
Cattura da eth0
Telefonia Wireless Strumenti Aiuto
eth0: <live capture in progress>
Pacchetti: 4903 · visualizzati: 4903 (100.0%)
Profilo: Default
CTRL (DESTRA)
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
┌──(marco㉿kali)-[/etc/network]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19
Nmap scan report for 192.168.50.101
Host is up (0.000065s 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
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:A0:26:54 (Oracle VirtualBox virt

Nmap done: 1 IP address (1 host up) scanned in 13.20 s

┌──(marco㉿kali)-[/etc/network]
└─$ nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19
16:43 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00025s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 13.12 s
econds

┌──(marco㉿kali)-[/etc/network]
└─$
```

```
on              Protocol  Length Info
.50.100         TCP         60 931 → 43408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 1005 → 57308 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101         TCP         74 44730 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 59912 → 9 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
.50.101         TCP         74 40050 → 524 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 57338 → 358 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.100         TCP         60 131 → 44730 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 9 → 59912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101         TCP         74 34270 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.100         TCP         60 524 → 40050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 358 → 57338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101         TCP         74 51328 → 310 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.100         TCP         60 681 → 34270 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 310 → 51328 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101         TCP         74 45088 → 151 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 44392 → 385 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 57534 → 849 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 33162 → 36 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
.50.100         TCP         60 151 → 45088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 385 → 44392 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 849 → 57534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 36 → 33162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.101         TCP         74 39806 → 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 33704 → 694 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.101         TCP         74 37778 → 38 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
.50.101         TCP         74 52350 → 386 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
.50.100         TCP         60 880 → 39806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 694 → 33704 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 38 → 37778 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
.50.100         TCP         60 386 → 52350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
                ICMPv6     118 Router Advertisement from e4:c3:2a:49:ac:34
st              ARP         60 Who has 192.168.1.100? Tell 192.168.1.103
st              ARP         60 Who has 192.168.1.101? Tell 192.168.1.103
.251            MDNS        87 Standard query 0x0000 PTR _spotify-connect._tcp.l
.255.250        SSDP       188 M-SEARCH * HTTP/1.1
.255.250        SSDP       188 M-SEARCH * HTTP/1.1
.255.250        SSDP       188 M-SEARCH * HTTP/1.1
captured (464 bits) on interface eth  0000  08 00 27 a0 26 54 08 00  27 f7 13
```

```
No mail.
msfadmin@metasploitable:~$ ifcpnfig
-bash: ifcpnfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:26:54
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: ::a00:27ff:fea0:2654/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea0:2654/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5452 (5.3 KB)  TX bytes:5452 (5.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24397 (23.8 KB)  TX bytes:24397 (23.8 KB)

msfadmin@metasploitable:~$ _
```

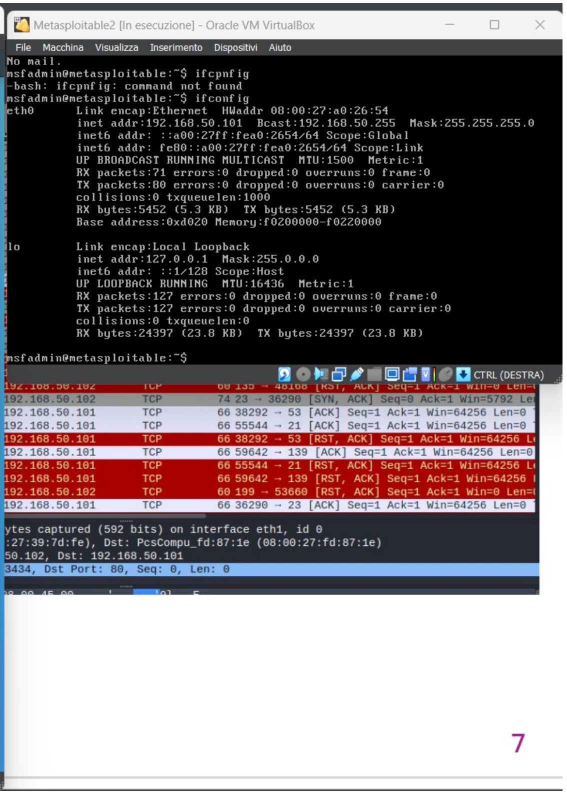
```
03 10:41 EDT
ers. Reverse DNS is disabled. Try using --system-dns

seconds
```


Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:46
Cattura da eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione … <Ctrl-/>
CTRL (DESTRA)

No.	Time	Source	Destination	Protocol	Length	Info
4361	559.999311250	192.168.50.101	192.168.50.100	TCP	60	552 → 60990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4362	559.999311294	192.168.50.101	192.168.50.100	TCP	60	538 → 41306 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4363	559.999311337	192.168.50.101	192.168.50.100	TCP	60	378 → 59674 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4364	559.999311367	192.168.50.101	192.168.50.100	TCP	60	616 → 47610 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4365	559.999323933	192.168.50.100	192.168.50.101	TCP	74	52524 → 202 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4366	559.999332467	192.168.50.100	192.168.50.101	TCP	74	60640 → 862 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4367	559.999359035	192.168.50.101	192.168.50.100	TCP	60	10 → 50958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4368	559.999359066	192.168.50.101	192.168.50.100	TCP	60	719 → 37562 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4369	559.999390211	192.168.50.101	192.168.50.100	TCP	60	202 → 52524 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4370	559.999390242	192.168.50.101	192.168.50.100	TCP	60	862 → 60640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4371	559.999399769	192.168.50.100	192.168.50.101	TCP	74	48286 → 360 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4372	559.999409075	192.168.50.100	192.168.50.101	TCP	74	60816 → 514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4373	559.999433300	192.168.50.100	192.168.50.101	TCP	74	60034 → 402 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4374	559.999441725	192.168.50.100	192.168.50.101	TCP	74	46640 → 388 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4375	559.999468788	192.168.50.101	192.168.50.100	TCP	60	360 → 48286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4376	559.999468840	192.168.50.101	192.168.50.100	TCP	74	514 → 60816 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
4377	559.999473416	192.168.50.100	192.168.50.101	TCP	66	60816 → 514 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
4378	559.999506620	192.168.50.101	192.168.50.100	TCP	60	402 → 60034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4379	559.999506651	192.168.50.101	192.168.50.100	TCP	60	388 → 46640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4380	559.999517531	192.168.50.100	192.168.50.101	TCP	74	46902 → 452 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4381	559.999526922	192.168.50.100	192.168.50.101	TCP	74	56170 → 48 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
4382	559.999551987	192.168.50.100	192.168.50.101	TCP	74	33738 → 337 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4383	559.999560366	192.168.50.100	192.168.50.101	TCP	74	35890 → 384 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4384	559.999591984	192.168.50.101	192.168.50.100	TCP	60	452 → 46902 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4385	559.999592016	192.168.50.101	192.168.50.100	TCP	60	48 → 56170 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4386	559.999615272	192.168.50.101	192.168.50.100	TCP	60	337 → 33738 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4387	559.999615303	192.168.50.101	192.168.50.100	TCP	60	384 → 35890 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4388	559.999664223	192.168.50.100	192.168.50.101	TCP	74	37994 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4389	559.999673256	192.168.50.100	192.168.50.101	TCP	74	57974 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4390	559.999698829	192.168.50.100	192.168.50.101	TCP	74	40706 → 253 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4391	559.999707816	192.168.50.100	192.168.50.101	TCP	74	47980 → 216 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4392	559.999740353	192.168.50.100	192.168.50.101	TCP	74	55054 → 932 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4393	559.999749319	192.168.50.100	192.168.50.101	TCP	74	60152 → 892 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4394	559.999775823	192.168.50.101	192.168.50.100	TCP	60	561 → 37994 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4395	559.999775855	192.168.50.101	192.168.50.100	TCP	60	769 → 57974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4396	559.999775900	192.168.50.101	192.168.50.100	TCP	60	253 → 40706 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4397	559.999775931	192.168.50.101	192.168.50.100	TCP	60	216 → 47980 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
Frame 129: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth   0000  08 00 27 a0 26 54 08 00  27 f7 13
```

eth0: <live capture in progress>   Pacchetti: 5100 · visualizzati: 5100 (100.0%)   Profilo: Default


Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
No mail.
msfadmin@metasploitable:~$ ifcpnfig
-bash: ifcpnfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:26:54
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: ::a00:27ff:fea0:2654/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fea0:2654/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5452 (5.3 KB)  TX bytes:5452 (5.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24397 (23.8 KB)  TX bytes:24397 (23.8 KB)

msfadmin@metasploitable:~$
```

```
192.168.50.102    TCP    74 23 → 36290 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
192.168.50.101    TCP    66 38292 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0
192.168.50.101    TCP    66 55544 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0
192.168.50.101    TCP    66 38292 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 L
192.168.50.101    TCP    66 59642 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0
192.168.50.101    TCP    66 55544 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 L
192.168.50.101    TCP    66 59642 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256
192.168.50.102    TCP    60 199 → 53660 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
192.168.50.101    TCP    66 36290 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0

ytes captured (592 bits) on interface eth1, id 0
:27:39:7d:fe), Dst: PcsCompu_fd:87:1e (08:00:27:fd:87:1e)
50.102, Dst: 192.168.50.101
3434, Dst Port: 80, Seq: 0, Len: 0
```

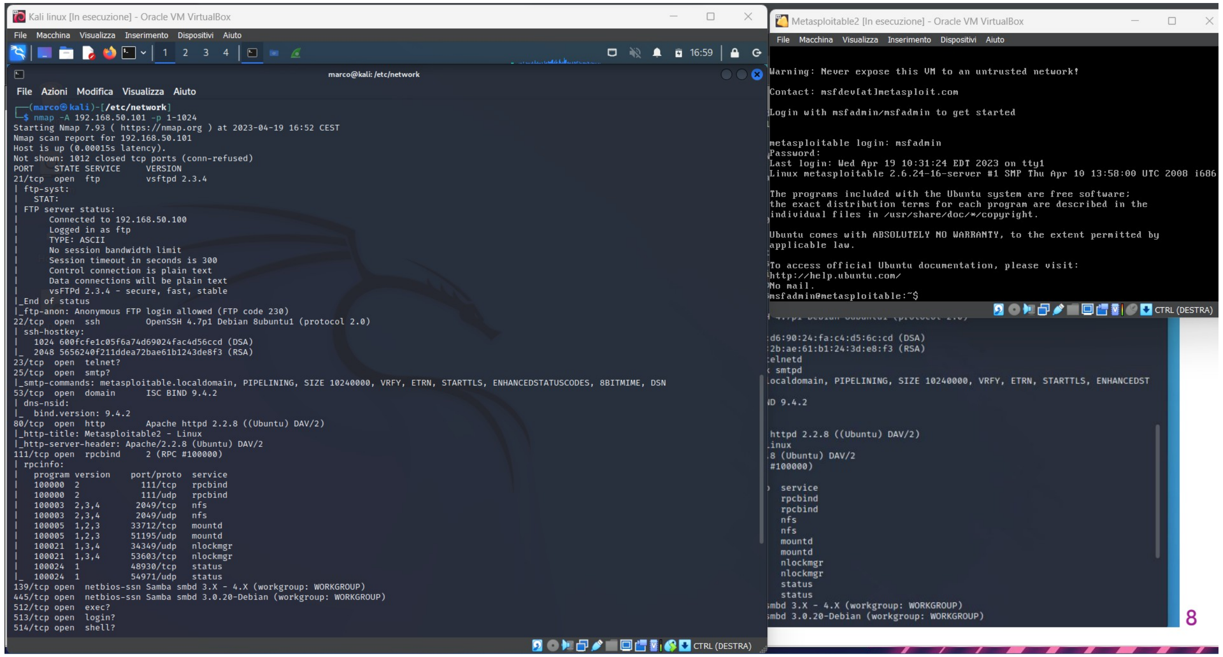
7

SCANSIONE NMAP -A Scan

TARGET METASPLOTABLE2 : 192.168.50.100
FONTE – Kali Linux : 192.168.50.101

```
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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)

23/tcp  open  telnet?

25/tcp  open  smtp?
|_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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

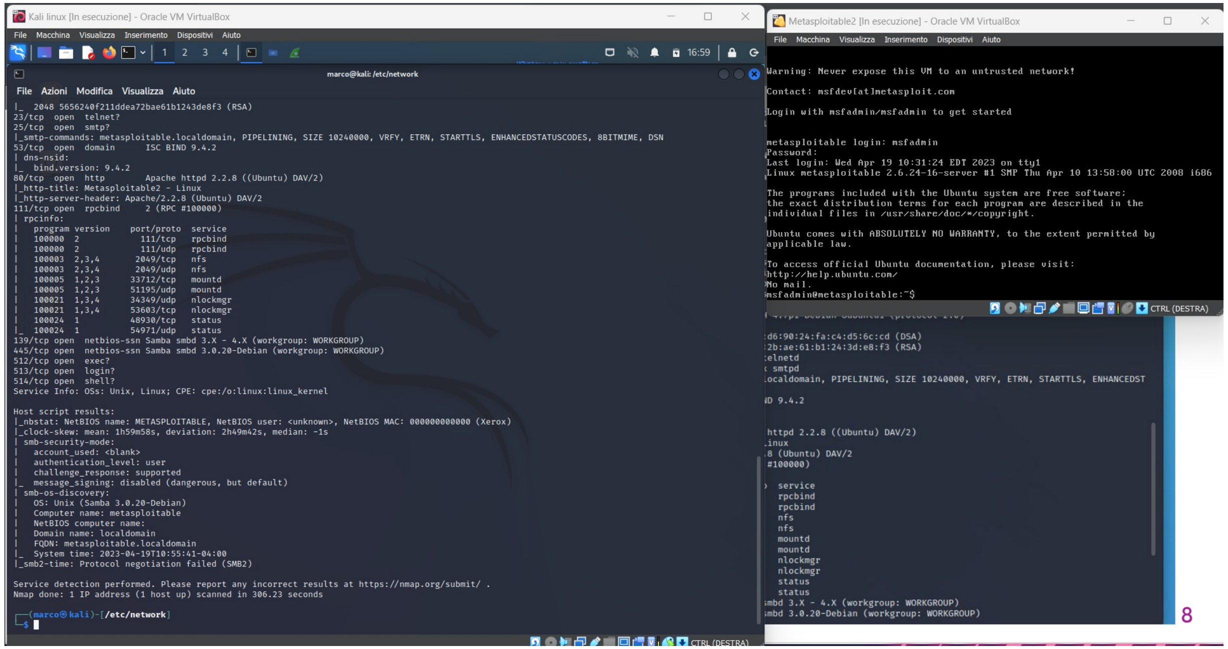
```
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      48360/udp   mountd
|   100005  1,2,3      49841/tcp   mountd
|   100021  1,3,4      41223/udp   nlockmgr
|   100021  1,3,4      43269/tcp   nlockmgr
|   100024  1          47729/tcp   status
|_  100024  1          54823/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?

513/tcp open  login?

514/tcp open  shell?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-04-19T13:56:48-04:00
|_clock-skew: mean: 2h00m11s, deviation: 2h50m00s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```


Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:59
marco@kali: /etc/network
File Azioni Modifica Visualizza Aiuto
CTRL (DESTRA)
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)
8

```
┌──(marco㉿kali)-[/etc/network]
└─$ nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-19 16:52 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00015s latency).
Not shown: 1012 closed tcp ports (conn-refused)
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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet?
25/tcp  open  smtp?
|_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)
|_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      33712/tcp   mountd
|   100005  1,2,3      51195/udp   mountd
|   100021  1,3,4      34349/udp   nlockmgr
|   100021  1,3,4      53603/tcp   nlockmgr
|   100024  1          48930/tcp   status
|_  100024  1          54971/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?
513/tcp open  login?
514/tcp open  shell?
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Apr 19 10:31:24 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

```
:d6:90:24:fa:c4:d5:6c:cd (DSA)
:2b:ae:61:b1:24:3d:e8:f3 (RSA)
telnetd
 smtpd
localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST

ND 9.4.2


 httpd 2.2.8 ((Ubuntu) DAV/2)
Linux
.8 (Ubuntu) DAV/2
 #100000)

   service
   rpcbind
   rpcbind
   nfs
   nfs
   mountd
   mountd
   nlockmgr
   nlockmgr
   status
   status
smbd 3.X - 4.X (workgroup: WORKGROUP)
smbd 3.0.20-Debian (workgroup: WORKGROUP)
```


Kali linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
16:59
marco@kali: /etc/network
File Azioni Modifica Visualizza Aiuto
CTRL (DESTRA)
Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)
8

```
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet?
25/tcp  open  smtp?
|_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)
|_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      33712/tcp   mountd
|   100005  1,2,3      51195/udp   mountd
|   100021  1,3,4      34349/udp   nlockmgr
|   100021  1,3,4      53603/tcp   nlockmgr
|   100024  1          48930/tcp   status
|_  100024  1          54971/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?
513/tcp open  login?
514/tcp open  shell?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s
| smb-security-mode:
|   account_used: <blank>
|   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: 2023-04-19T10:55:41-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 306.23 seconds

┌──(marco㉿kali)-[/etc/network]
└─$ 
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Apr 19 10:31:24 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

```
:d6:90:24:fa:c4:d5:6c:cd (DSA)
:2b:ae:61:b1:24:3d:e8:f3 (RSA)
telnetd
 smtpd
localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDST

ND 9.4.2


 httpd 2.2.8 ((Ubuntu) DAV/2)
Linux
.8 (Ubuntu) DAV/2
 #100000)

   service
   rpcbind
   rpcbind
   nfs
   nfs
   mountd
   mountd
   nlockmgr
   nlockmgr
   status
   status
smbd 3.X - 4.X (workgroup: WORKGROUP)
smbd 3.0.20-Debian (workgroup: WORKGROUP)
```