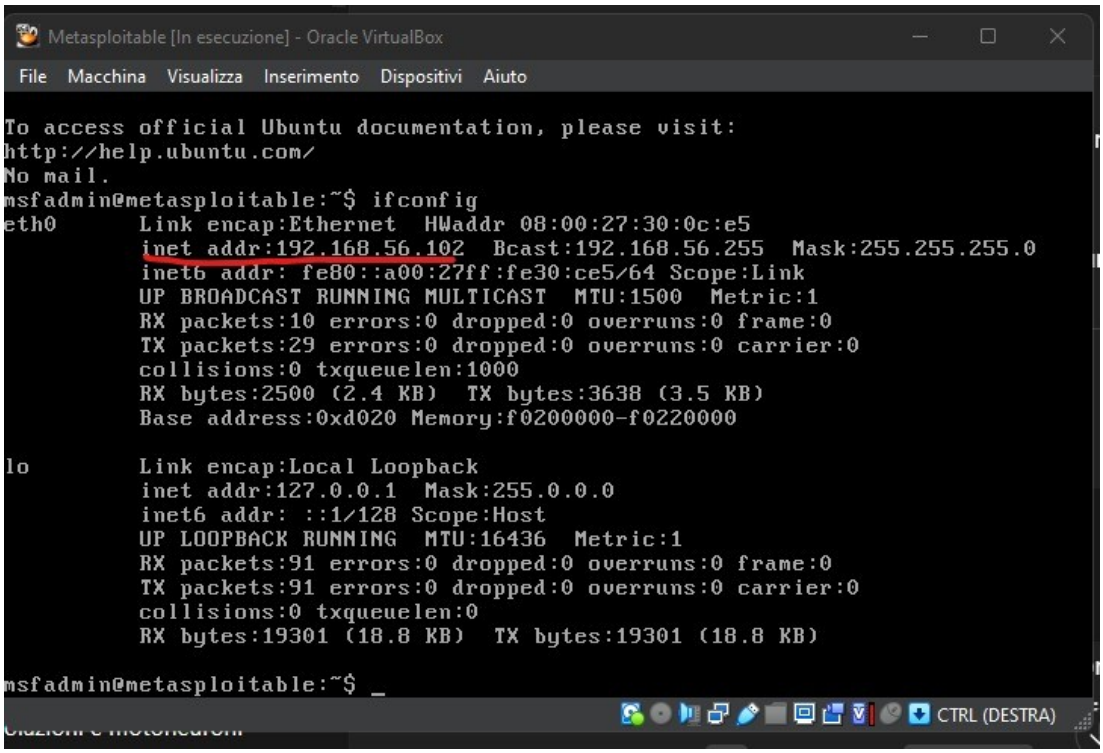
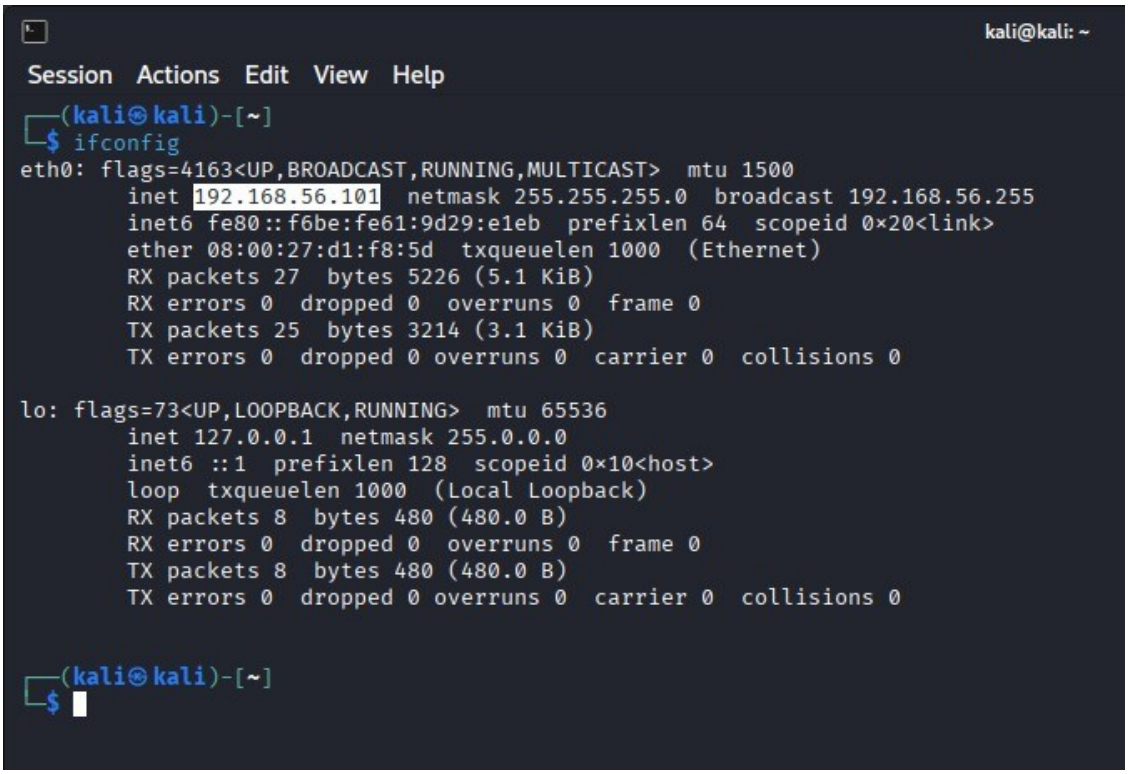
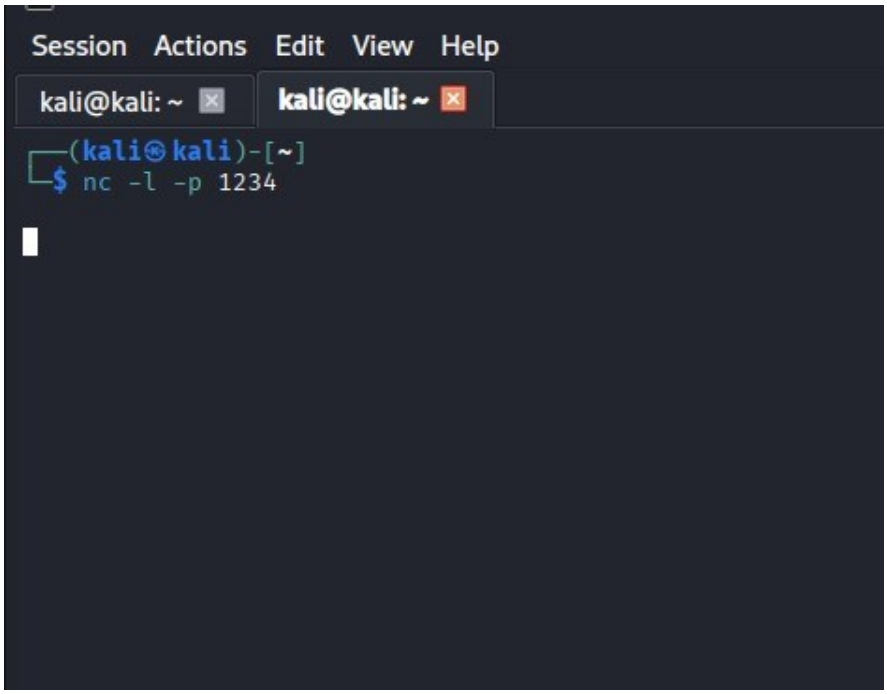
W9D1 – FRANCESCO MONTALTO

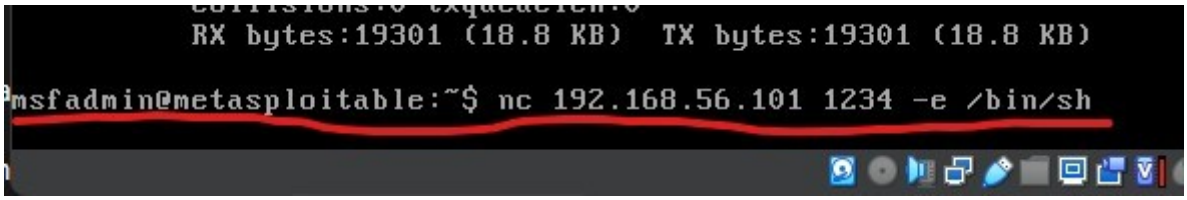
1. Innanzitutto mi sono procurato i relativi IP di Meta e Kali, e ne ho preso nota.





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





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.

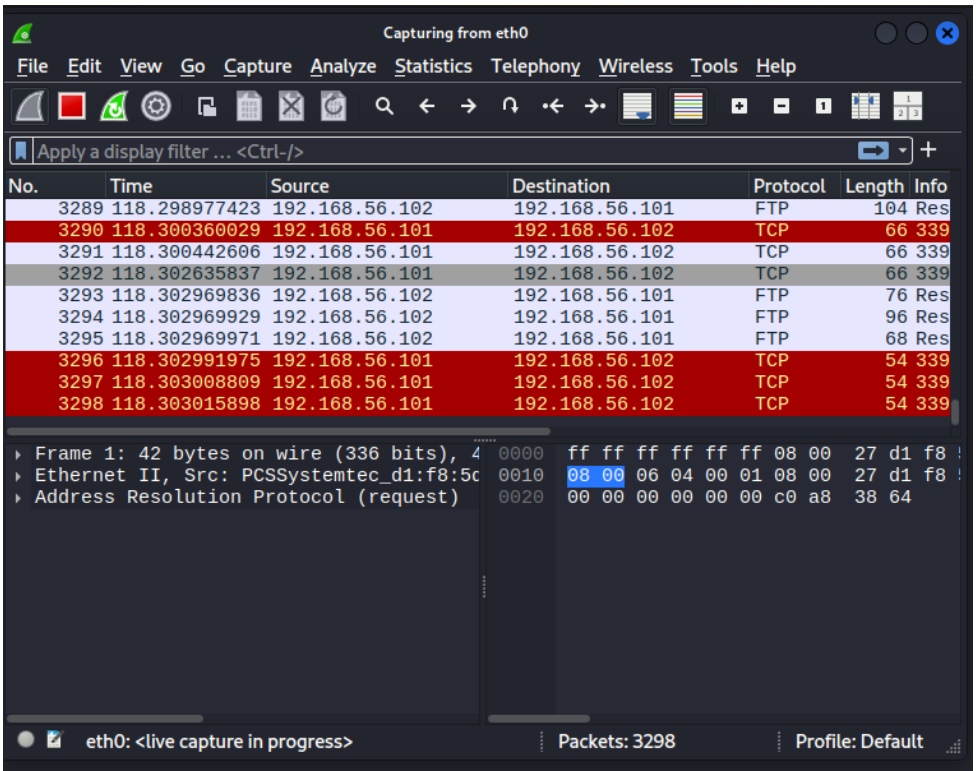
```
┌──(kali㉿kali)-[~]
└─$ nc -l -p 1234

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.

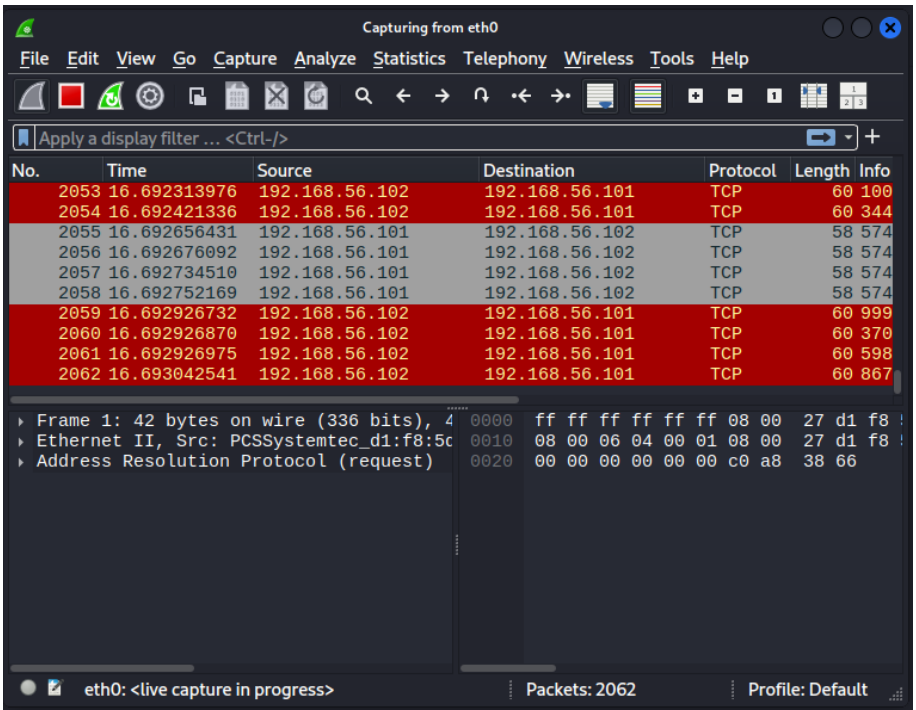
5. SCANSIONE TCP SULLE PORTE WELL KNOWN

```
┌──(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
```

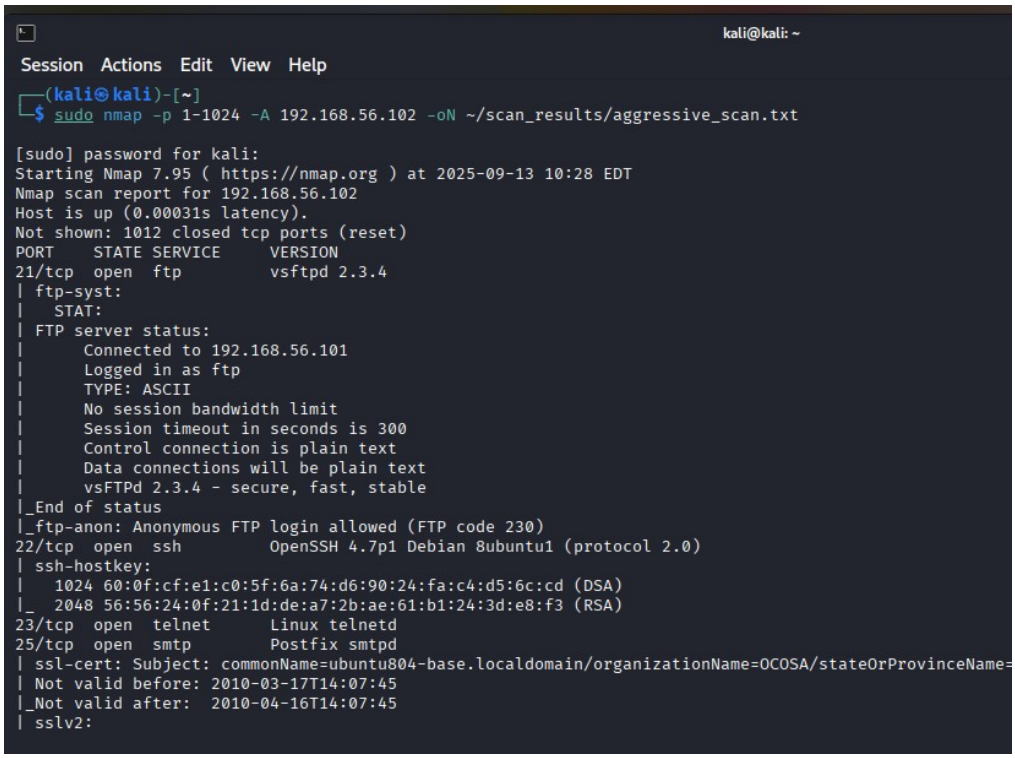


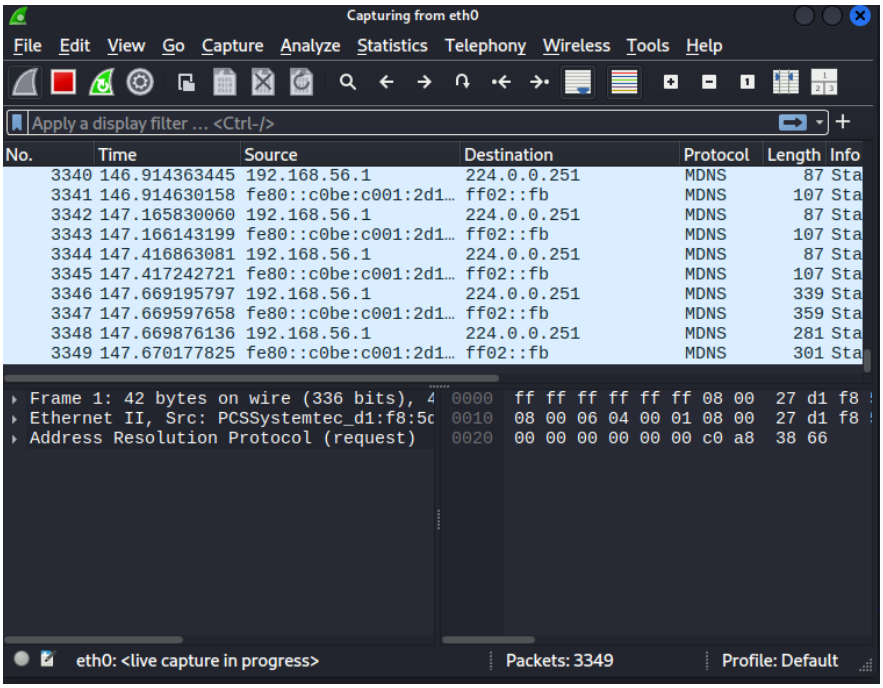
6. SCANSIONE SYN SULLE PORTE WELL KNOWN

```
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
```



7. SCANSIONE SWITCH -A SULLE PORTE WELL KNOWN





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).

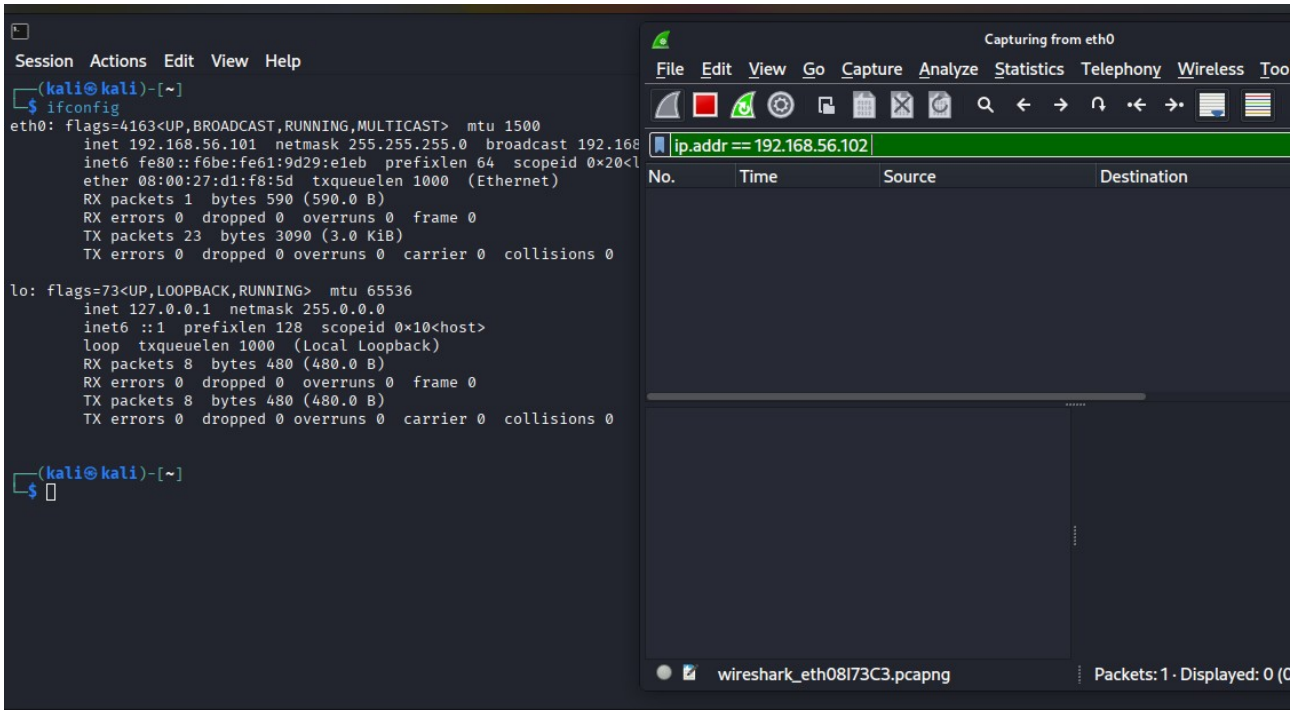
SCANSIONE SYN	RISULTATO
FONTE	Kali 192.168.56.101
TARGET	Metasploitable 192.168.56.102
TIPO DI SCAN	SYN Scan (`sudo nmap -sS -p 1-1024`)
RISULTATI OTTENUTI	21/tcp ftp,22/tcp ssh,23/tcp telnet,25/tcp smtp,53/tcp domain,80/tcp http,111/tcp rpcbind,139/tcp netbios-ssn,445/tcp microsoft-ds,512/tcp exec,513/tcp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

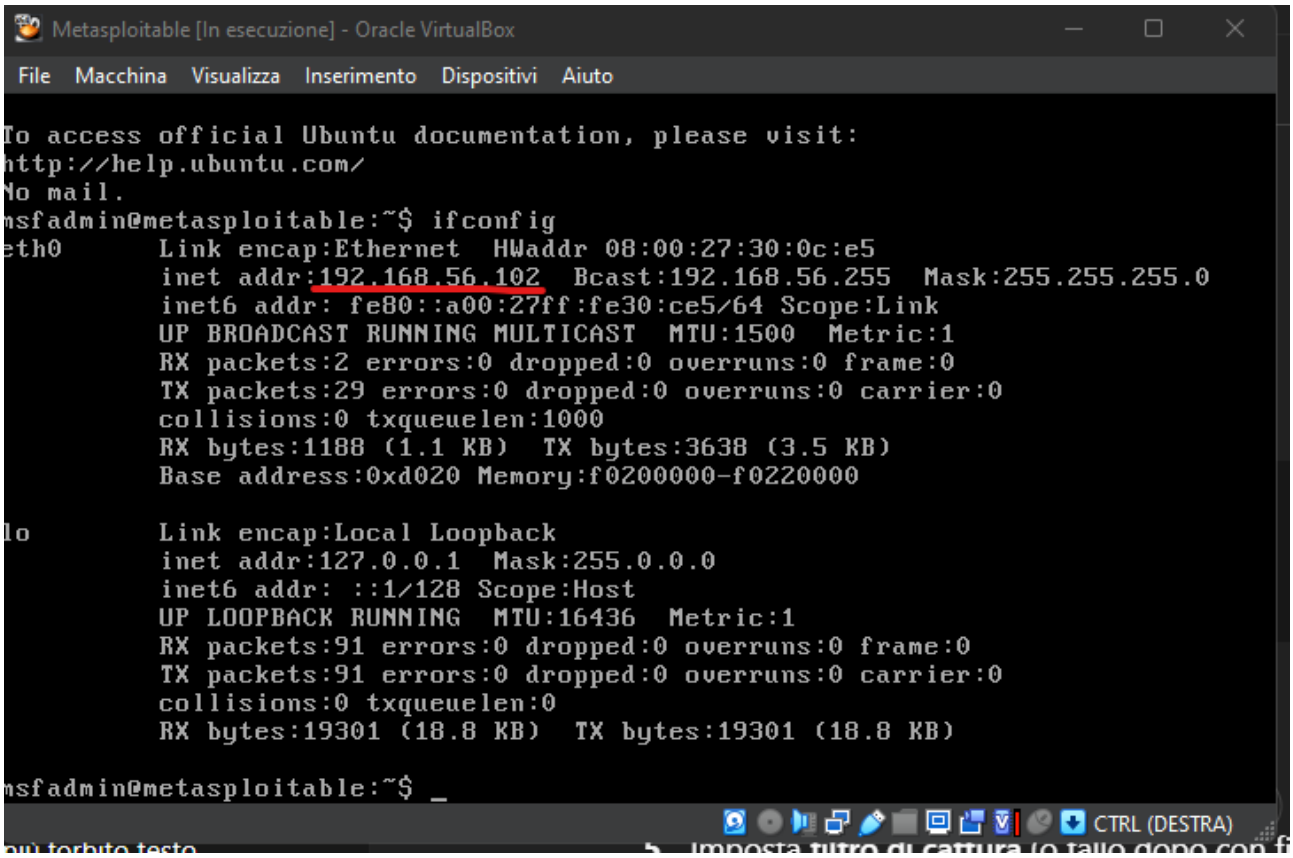
SCANSIONE AGGRESSIVE	RISULTATO
FONTE	Kali 192.168.56.101
TARGET	Metasploitable 192.168.56.102
TIPO DI SCAN	Aggressive Scan (sudo nmap -p 1-1024 -A)
RISULTATI OTTENUTI	21/tcp = ftp, vsftpd 2.3.4, login anonimo permesso 22/tcp = ssh, OpenSSH 4.7p1 Debian 8ubuntu1 (DSA/RSA hostkeys) 23/tcp = telnet, Linux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

ESERCIZIO FACOLTATIVO:

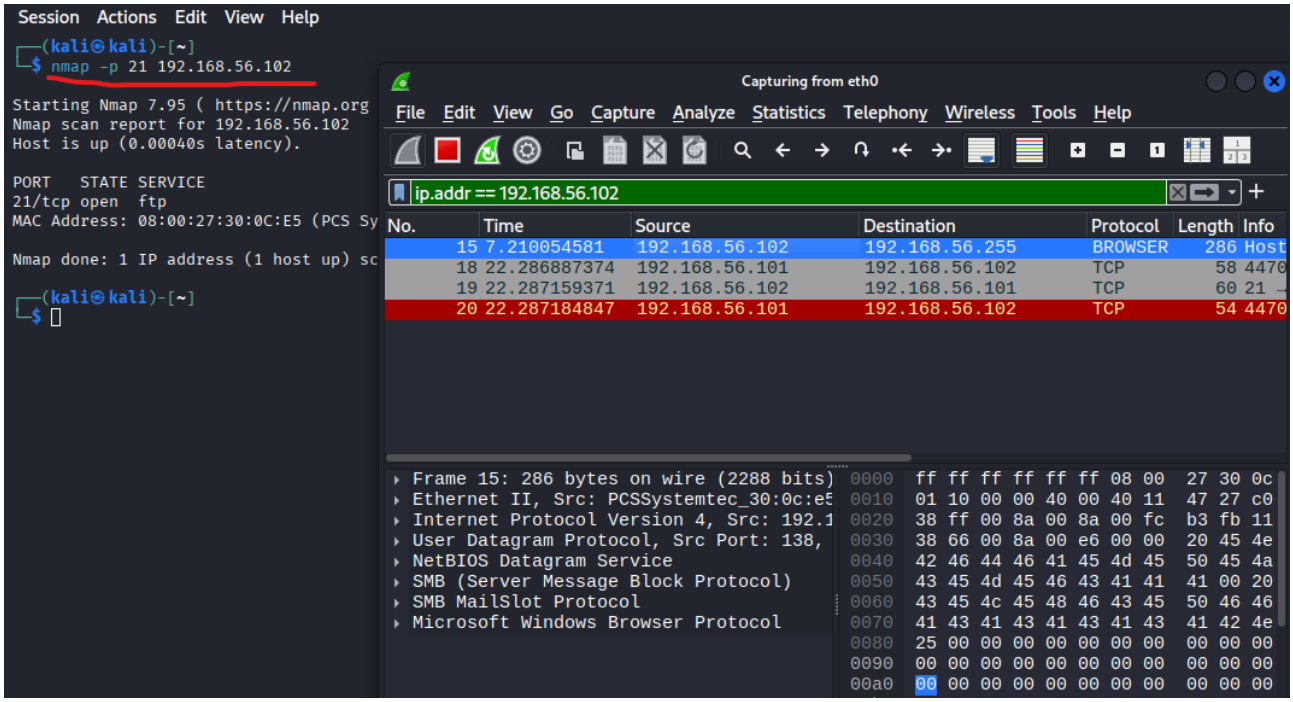
Lo scopo di questa parte è evidenziare la differenza tra una scansione TCP completa (TCP Connect) e una scansione SYN (stealth), intercettando e analizzando i pacchetti inviati dalla macchina sorgente tramite Wireshark.

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

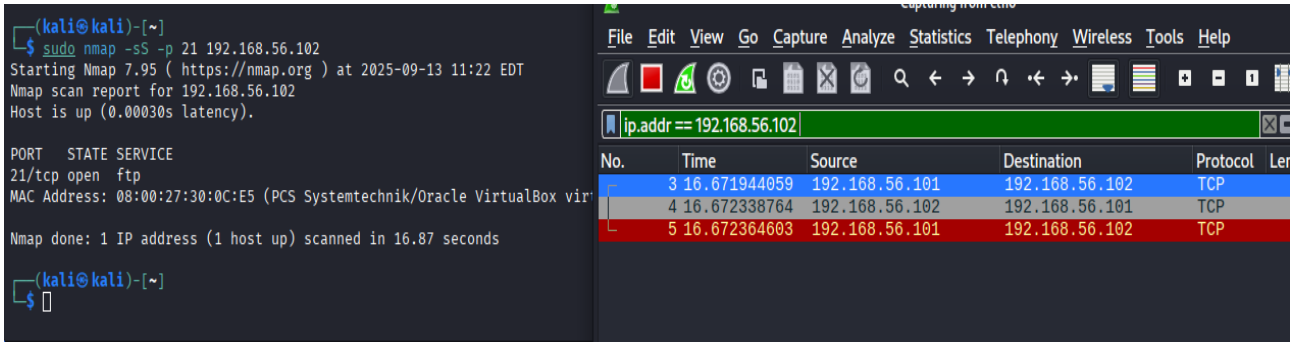




2. Ho eseguito il TCP, dopo aver premuto “Start” su Wireshark, ed ho visionato i pacchetti. La connessione viene completata interamente. Questo rende la scansione più semplice da rilevare nei log del server, perché il servizio FTP riceve una connessione reale.

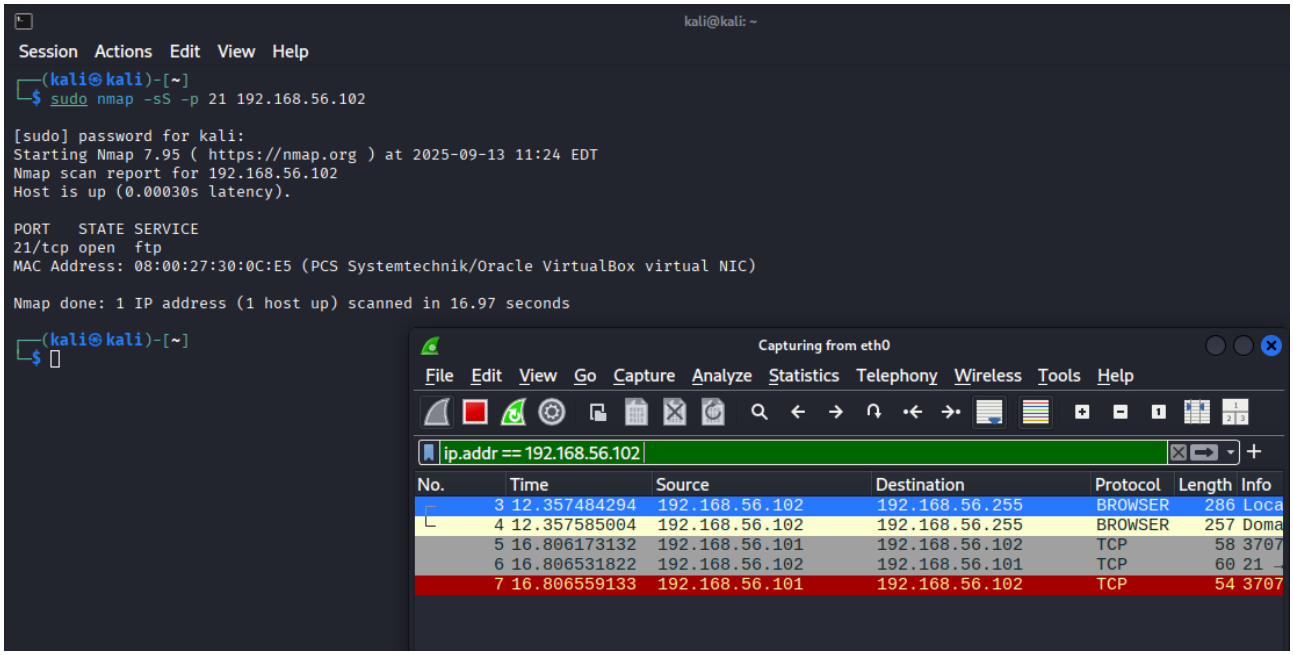


3. Ho premuto nuovamente “Start” su Wireshark, e stavolta ho eseguito il SYN su Kali.



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



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.