

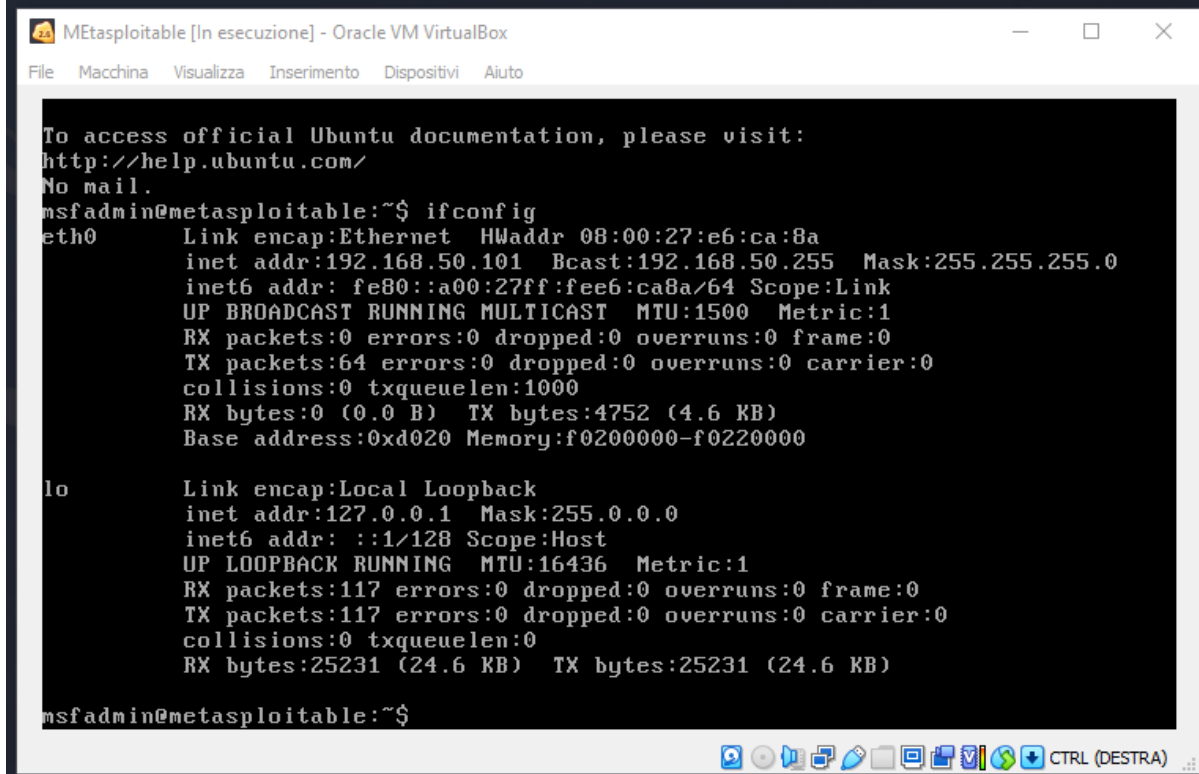
Nmap

Obiettivi: Utilizzare il software NMap per scansionare la macchina metasploitable.

1) Host Discovery

```
(root@kali)-[/home/kali]
# nmap -sL 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:19 EDT
Nmap scan report for 192.168.50.101
Nmap done: 1 IP address (0 hosts up) scanned in 13.05 seconds

(root@kali)-[/home/kali]
# nmap -sn 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:20 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00039s latency).
MAC Address: 08:00:27:E6:CA:8A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```



The screenshot shows a window titled "MEtasploitable [In esecuzione] - Oracle VM VirtualBox". The window contains a terminal window with the following output:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:ca:8a
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee6:ca8a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4752 (4.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

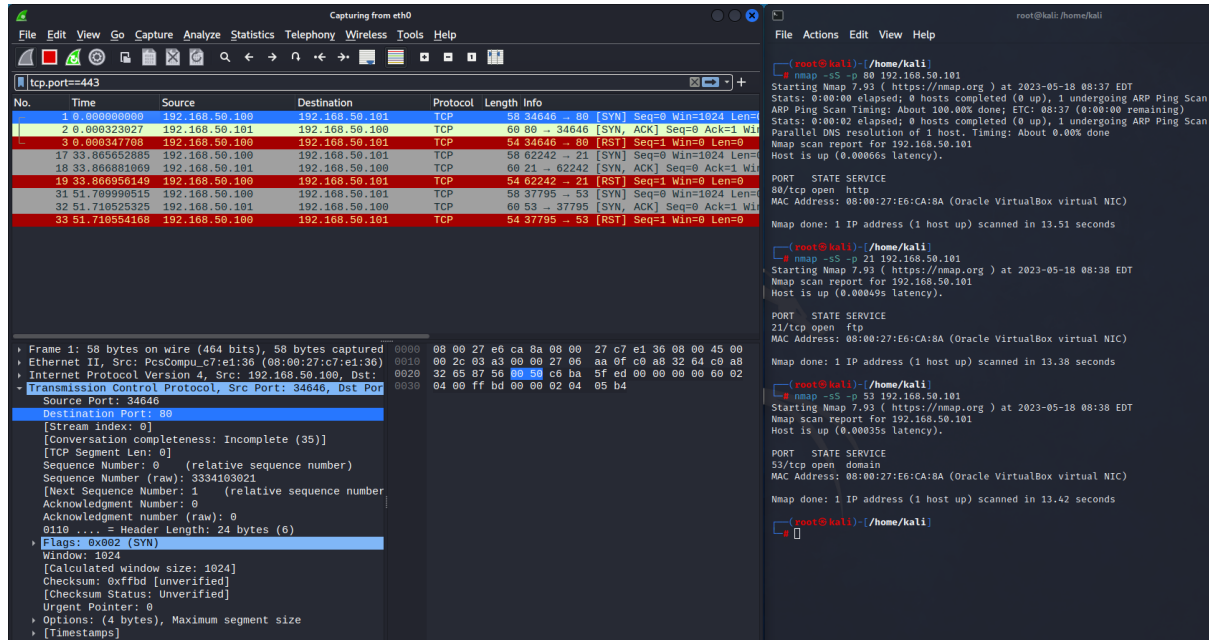
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25231 (24.6 KB)  TX bytes:25231 (24.6 KB)

msfadmin@metasploitable:~$
```

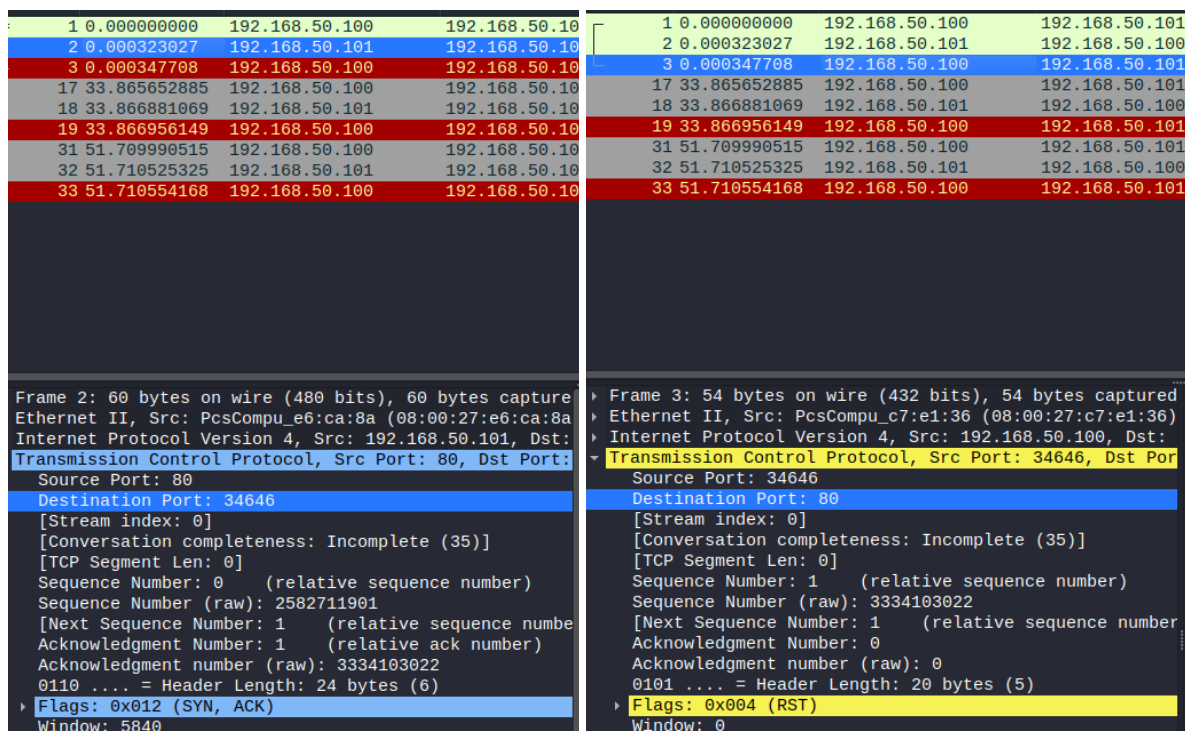
Ho innanzitutto elevato i privilegi dell'utente Kali a **root** utilizzando il comando **sudo su** per così utilizzare **NMap**. Successivamente ho ricercato l'host da "attaccare" usando il comando **nmap -sn** e indicando l'indirizzo IP della macchina da analizzare. In questo caso l'indirizzo 192.168.50.101 mi ha confermato che l'host è operativo (Host is up).

2) Scansione SYN

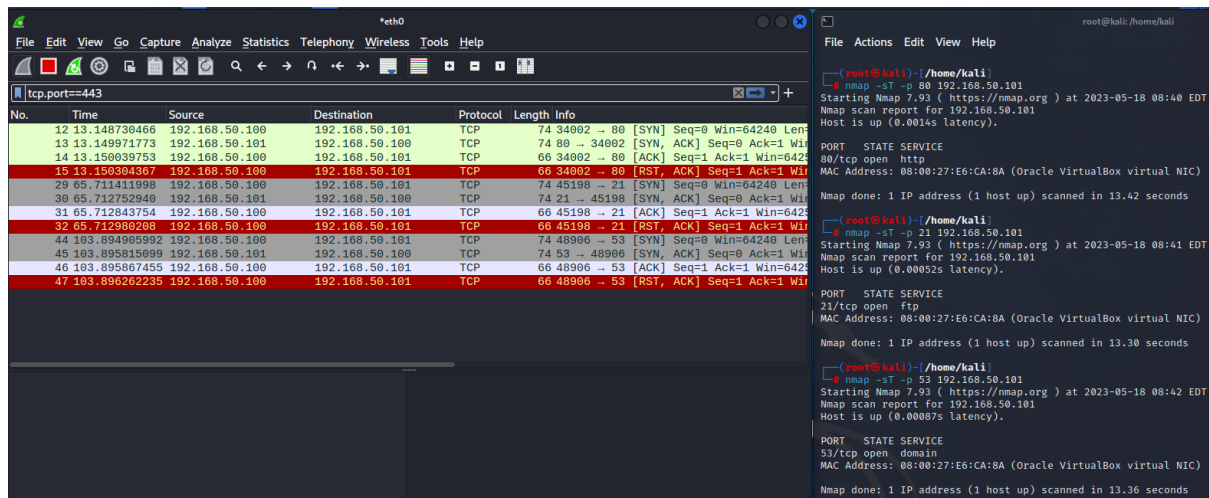
Con il comando ***nmap -sS*** ho analizzato 3 porte Well Known casuali aperte e ho catturato con **Wireshark** lo scambio di pacchetti che è avvenuto tra **Kali** e **Metasploitable**.



La scansione **SYN** è un metodo meno invasivo rispetto al successivo che ho tentato. In questo metodo **NMap** una volta ricevuto il pacchetto **SYN / ACK** da **Metasploitable** non conclude quello che viene chiamato il **3-way-handshake**. Una volta che la porta viene dichiarata aperta **NMap** tronca la comunicazione.



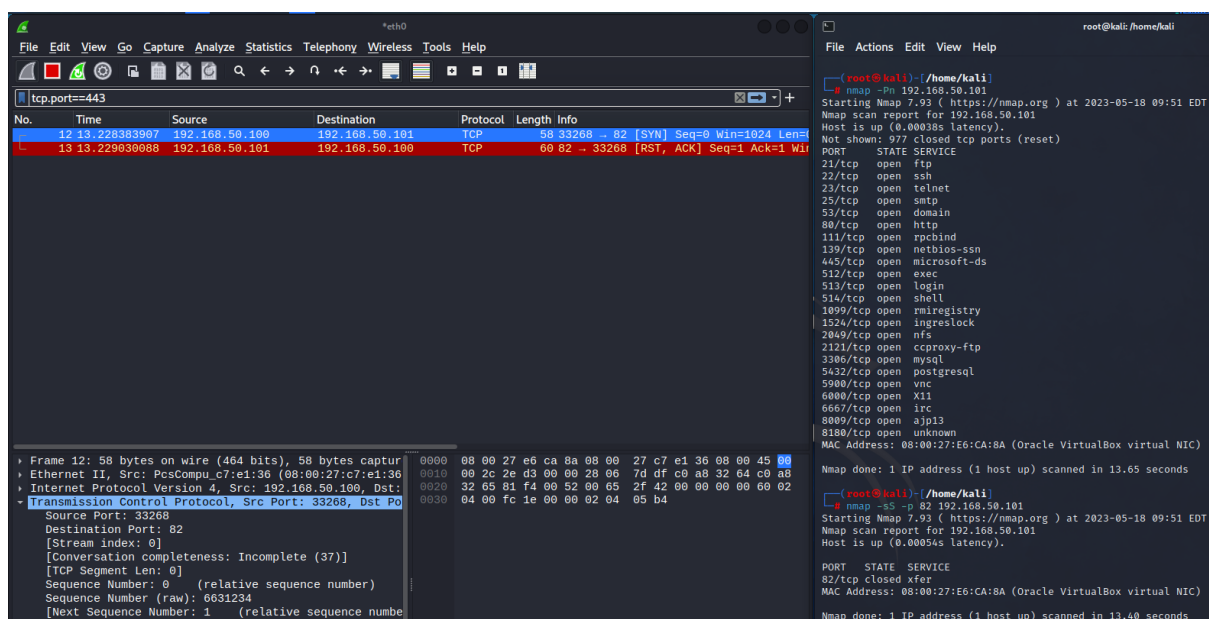
3) Scansione TCP



La Scansione **TCP** invece è un metodo più invasivo. Utilizzando il comando ***nmap -sT*** il programma cerca di concludere con la macchina bersaglio la **Stretta di Mano in 3 Passaggi** stabilendo quindi un canale per lo scambio di pacchetti. Perciò confrontando le due figure e utilizzando il filtro per controllare i protocolli TCP in questo metodo c'è un pacchetto in più perchè il terzo passaggio non viene interrotto da Nmap.

4) Scansione Porte Chiuse

Ho utilizzato il comando ***nmap -Pn*** per ricercare tutti gli host attivi del bersaglio e successivamente analizzare lo scambio di pacchetti con una porta chiusa per vedere cosa succedesse su *Wireshark*.



Ovviamente alla prima richiesta di **NMap** la connessione viene resettata essendo la porta inattiva a differenza di quelle aperte.

5) Scansione Aggressiva

La **Scansione Aggressiva** viene utilizzata per fare un controllo più approfondito del bersaglio inviando un grandissimo numero di pacchetti ma ha come contro il fatto che è facilmente individuabile dai sistemi di sicurezza. Questo tipo di scansione offre inoltre altre opzioni di **NMap** come lo scoprire il Sistema Operativo del bersaglio o l'utente attualmente collegato.

The image shows two windows side-by-side. The left window is Wireshark, displaying a packet capture on the 'eth0' interface. It shows a large number of TCP packets (RST, ACK) sent to 192.168.50.101 from 192.168.50.100. The right window is a terminal running Nmap. The command is 'nmap -A -p 15-515 192.168.50.101'. The output shows that the host is up, and it lists various open ports and services, including 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 443/tcp (https), 445/tcp (smb), 513/tcp (login), and 514/tcp (shell). It also identifies the operating system as Linux 2.6.9 - 2.6.33.

Nella figura a sinistra possiamo vedere una piccolissima parte di tutti i pacchetti inviati da **NMap** (2471 pacchetti); a destra e sotto invece le porte aperte, i processi attivi per ogni porta, informazioni sul Sistema Operativo di **Metasploitable** e altro.

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2023-05-18T08:47:17-04:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 1h59m58s, deviation: 2h49m43s, median: -2s
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT ADDRESS
1 0.63 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 102.46 seconds
```