

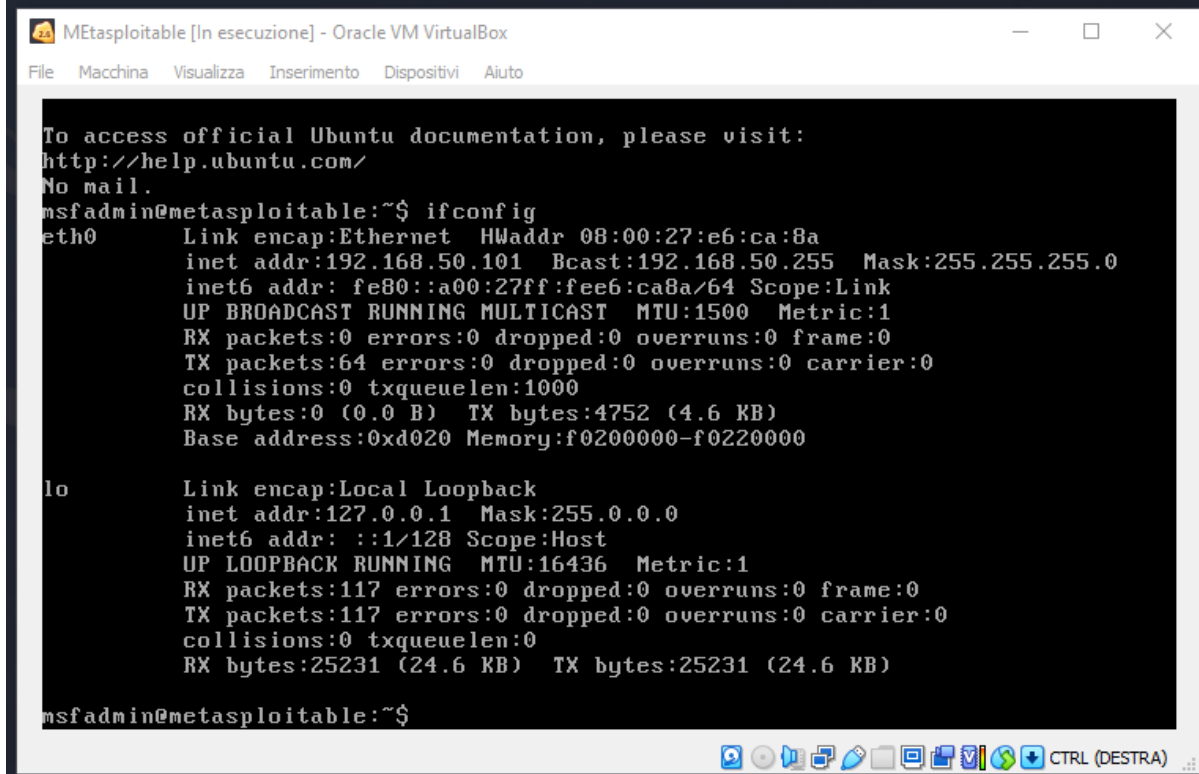
Nmap

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

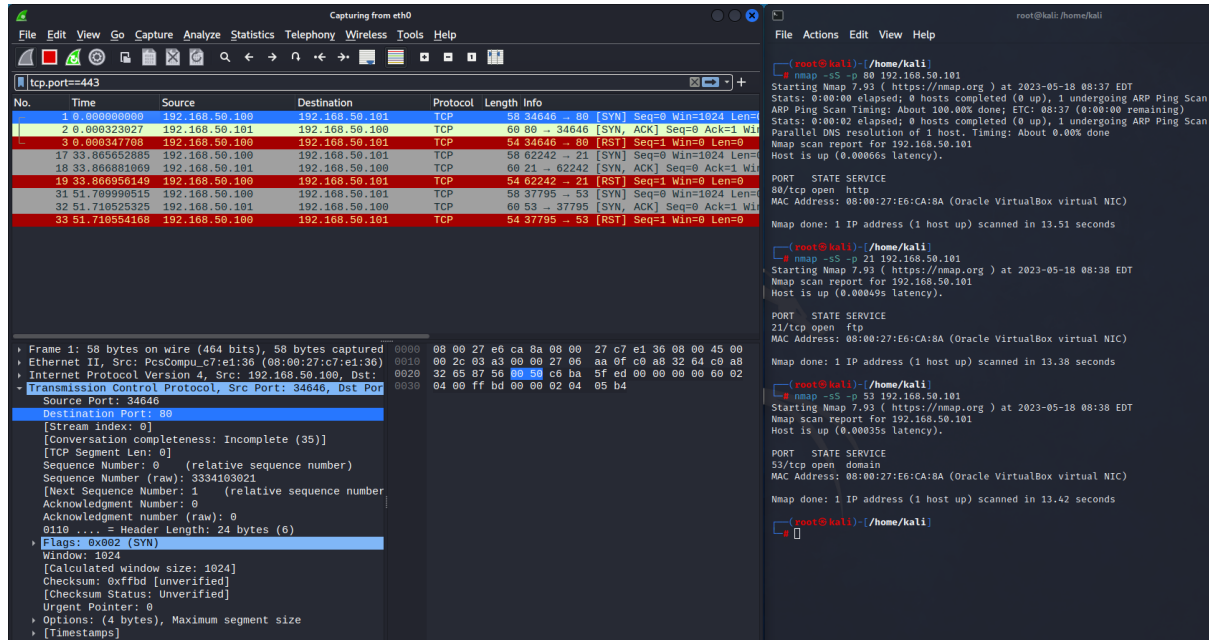
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0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

msfadmin@metasploitable:~$
```

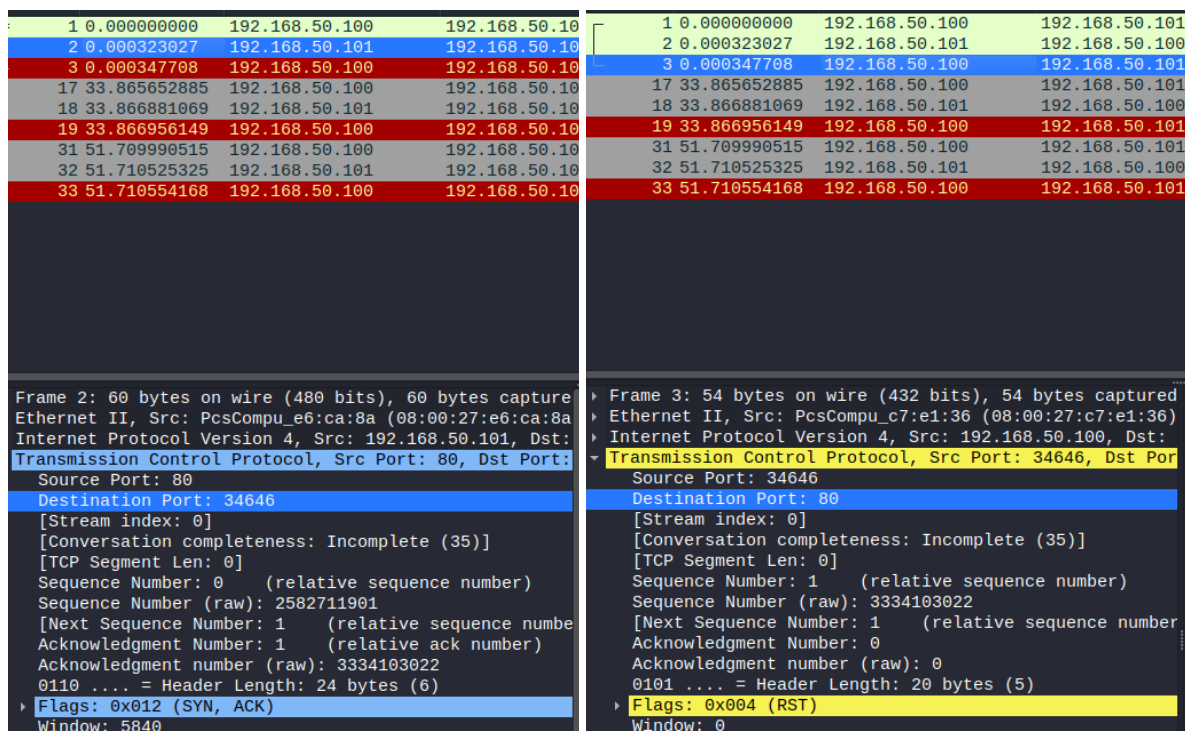
Ho innanzitutto elevato i privilegi dell'utente Kali a **root** utilizzando il comando **sudo su** per così utilizzare **NMap**. Successivamente ho ricercato l'host da "attaccare" usando il comando **nmap -sn** e indicando l'indirizzo IP della macchina da analizzare. In questo caso l'indirizzo 192.168.50.101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

2) Scansione SYN

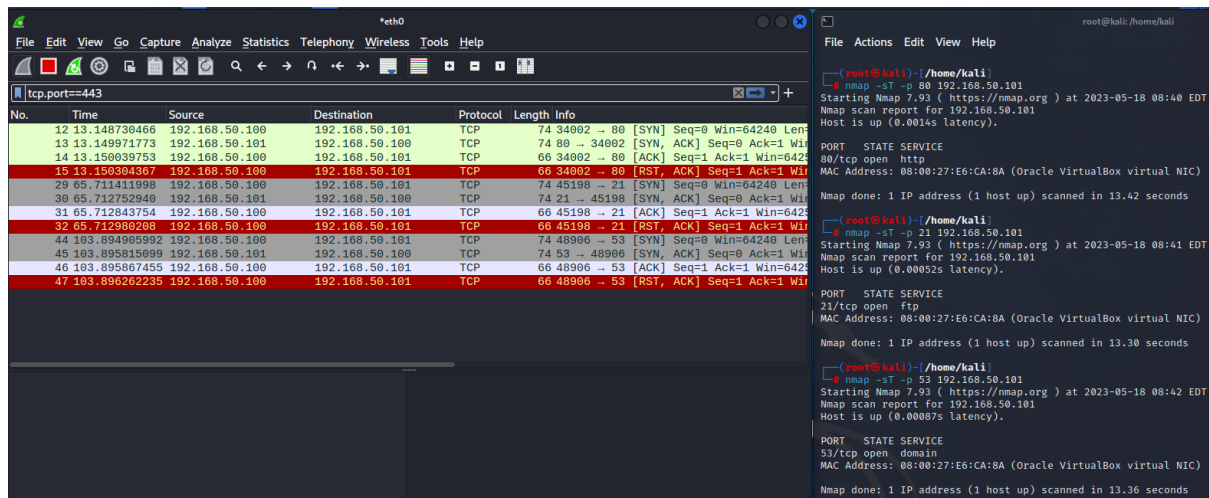
Con il comando ***nmap -sS*** ho analizzato 3 porte Well Known casuali aperte e ho catturato con **Wireshark** lo scambio di pacchetti che è avvenuto tra **Kali** e **Metasploitable**.



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.



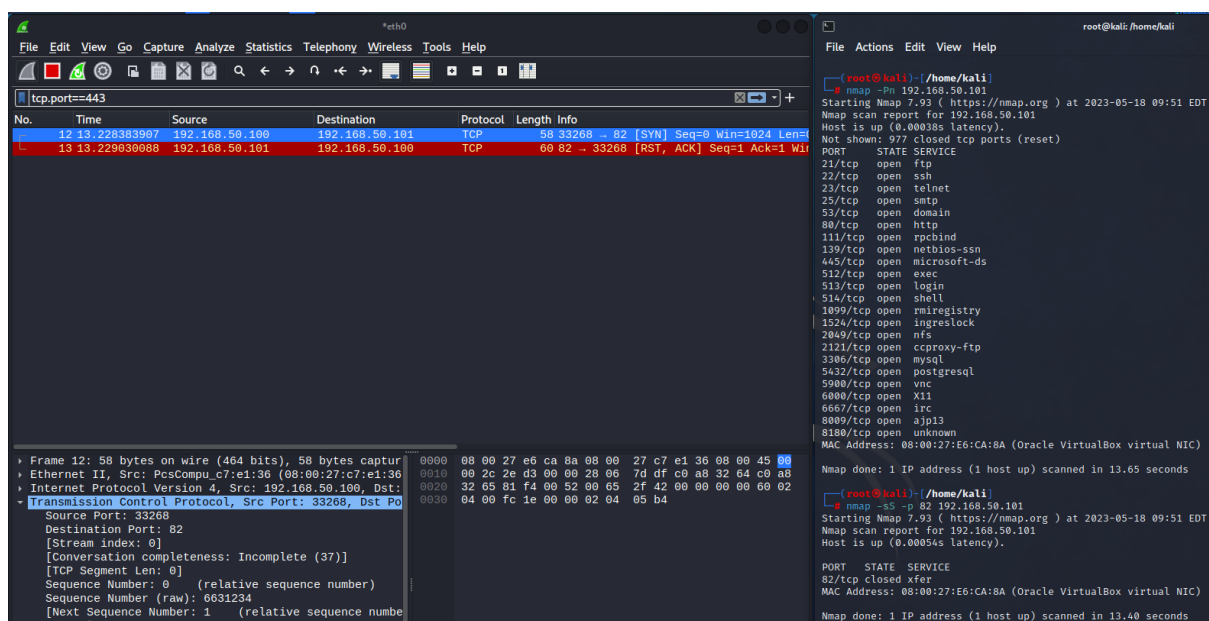
3) Scansione TCP



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 screenshot displays the Nmap interface. The left pane shows a list of packets sent during the scan, including their sequence numbers, times, sources, destinations, protocols, lengths, and information. The right pane shows the scan output, including the starting Nmap version, the target IP address, the scan results for various ports, and the OS detection results.

Destination Port: 419
[Stream index: 426]
[Conversation completeness: Incomplete (37)]
[TCP segment len: 6]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1557670747
[Next Sequence Number: 1 (relative sequence number)
Acknowledgment Number: 0
Acknowledgment Number (raw): 0

Destination Port (tcp.dstport), 2 bytes | Packets: 2471 | Displayed: 2471 (100.0%) | Profile: Default

File Actions Edit View Help
root@kali: /home/kali
Starting Nmap 7.93 (https://nmap.org) at 2023-05-18 08:46 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00063s latency).
Not shown: 489 closed tcp ports (reset)
PORT STATE SERVICE
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-ann: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 608f9efc1c056a74d69024facd56cdd (DSA)
| 2048 5656240f21ddea72bae61b1243d8f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_ smtp-command: metasplitable.localdomain, PIPELINING, SIZE 10240000, VR
ATUSCODES, 8BITIME, 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 3067/udp mountd
| 100005 1,2,3 4750/tcp mountd
| 100021 1,3,4 5696/udp nlockmgr
| 100021 1,3,4 5761/udp nlockmgr
| 100024 1 50901/tcp status
| 100024 1 56748/udp status
139/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login? Netkit rshd
514/tcp open shell Netkit rshd
MAC Address: 08:00:27:E6:CA:8A (Oracle VirtualBox virtual NIC)

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: metasplitable.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: metasplitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasplitable.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
```