Traccia:

Vedremo da vicino nmap e i suoi comandi. Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:-

Scansione TCP sulle porte well-known
-Scansione SYN sulle porte well-known
-Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

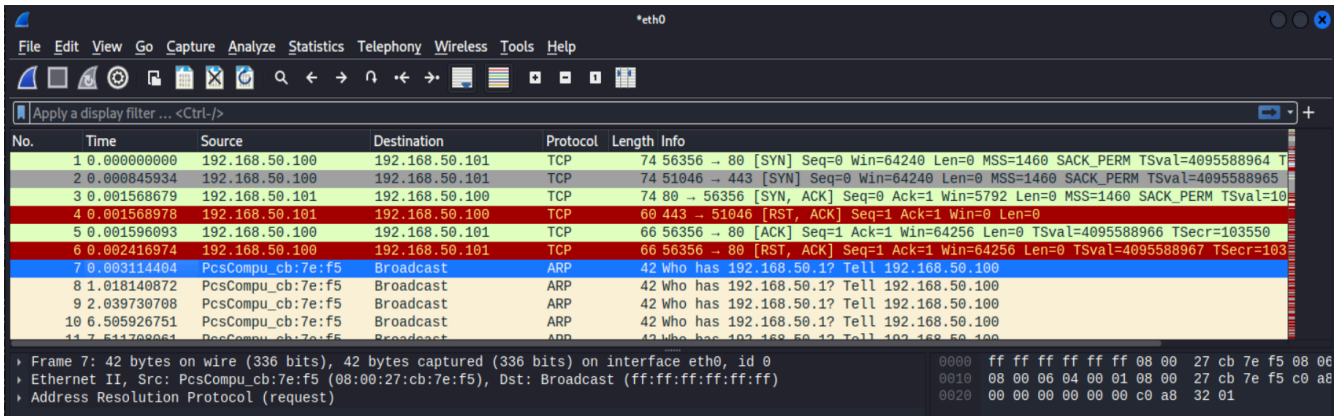
Svolgimento:

Nelle due immagini qui sotto si evidenzia come la scansione TCP (nmap -sT) sulle porte aperte come ad esempio la porta 80, completi il three way hankshake

Righe 1 – 3 – 5 del file di cattura

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p 1-1024 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 10:14 EST
Nmap scan report for 192.168.50.101
Host is up (0.0020s 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 13.25 seconds
```



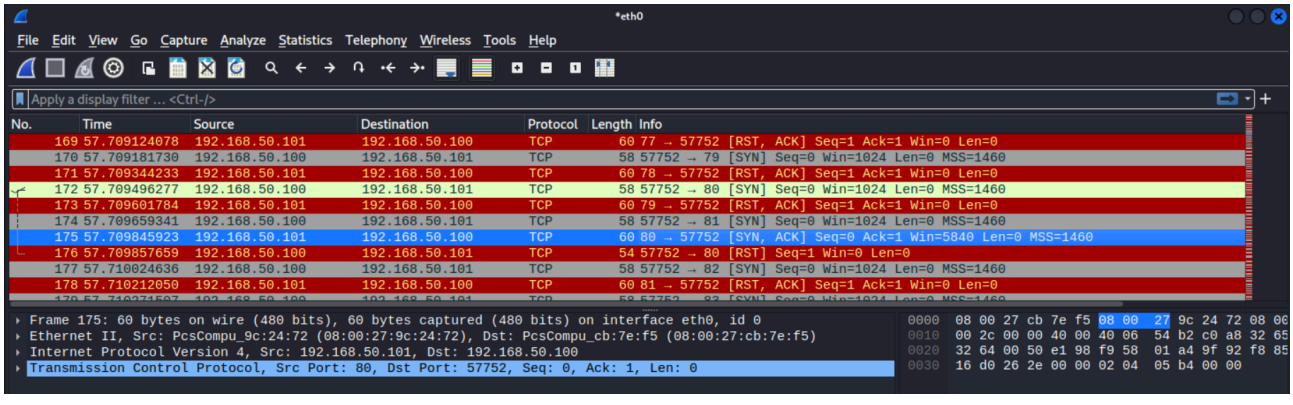
Nelle due immagini qui sotto si evidenzia come la scansione SYN (nmap -sS) sulle porte aperte come ad esempio la porta 80, NON completi il three way hankshake

Righe 172 – 175 – 176 del file di cattura

Con l'aggiunta dell'opzione -r le porte vengono testate in ordine

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -r -p 1-1024 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 10:35 EST
Nmap scan report for 192.168.50.101
Host is up (0.00040s 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: 08:00:27:9C:24:72 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -r -p 1-1024 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 10:43 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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 192.168.50.100
|      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 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
|_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      34561/tcp   mountd
|   100005  1,2,3      38843/udp   mountd
|   100021  1,3,4      41804/udp   nlockmgr
|   100021  1,3,4      54101/tcp   nlockmgr
|   100024  1          49275/tcp   status
|_  100024  1          51154/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  Detbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:9C:24:72 (Oracle VirtualBox virtual NIC)
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:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-30T10:43:54-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h29m46s, deviation: 3h32m25s, median: -26s

TRACEROUTE
HOP RTT     ADDRESS
```

FONTE DELLO SCAN:
Servizio nmap con diverse opzioni utilizzate dalla macchina Kali Linux 192.168.50.100 rete internal

TARGET DELLO SCAN:
Macchina Metaslpoitable2 indirizzo 192.168.50.100 rete internal

TIPO DI SCAN:
nmap con opzione -A che offre tutte le informazioni sul sistema della macchina target

RUSULTATI OTTENUTI:
Porte aperte con i servizi attivi, nome computer, tipo di sistema operativo, dominio di appartenenza, tipo di host e livello di autenticazione.