Traccia Nmap:

Sulle base delle nozioni viste, eseguire diversi tipi di scan sulla macchine metasploitable con nmap, come di seguito:

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

La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine.
E' molto importante in questa fase essere organizzati e strutturati.
Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report in Pdf (tabella su word ad esempio) che riporti in maniera chiara:

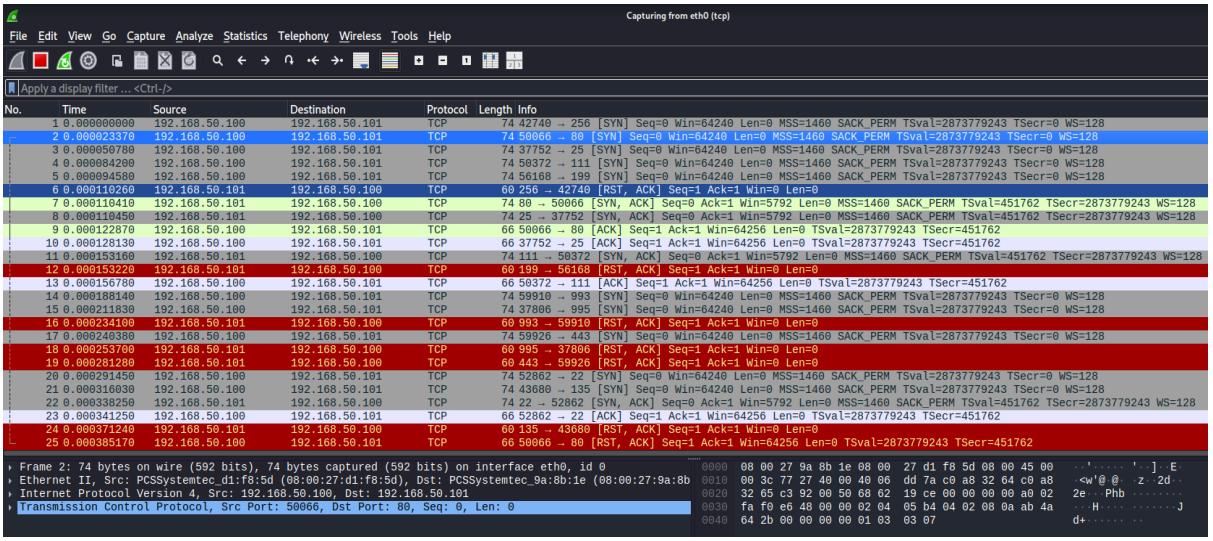
- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

SVOLGIMENTO:

scansione TCP sulle porte well- known

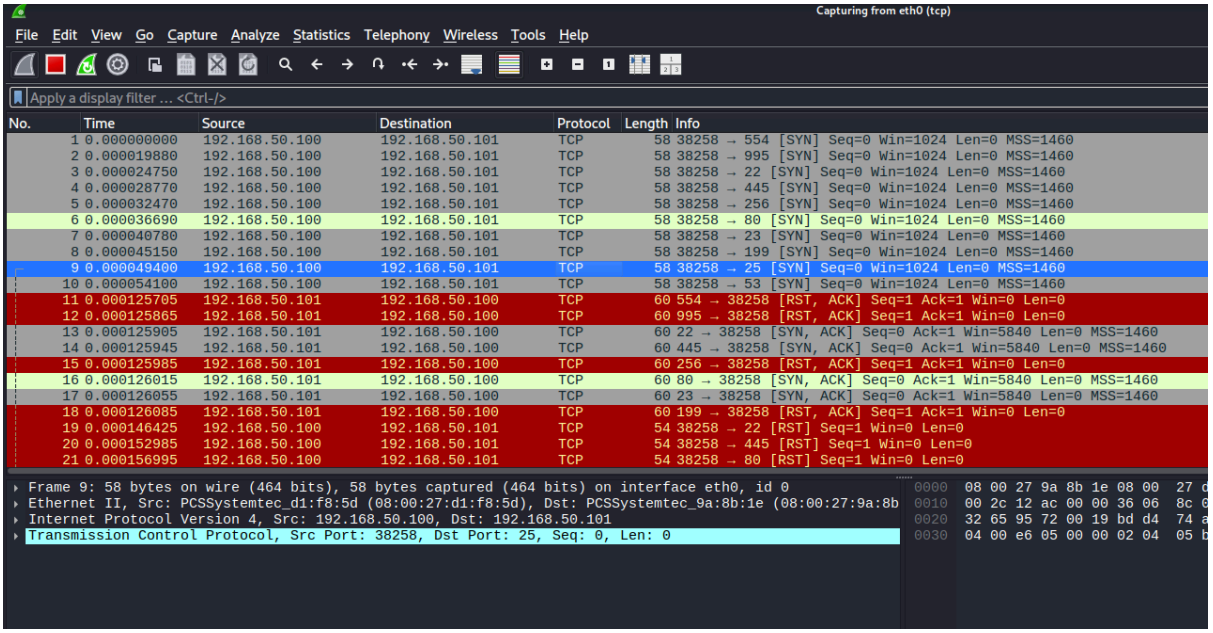
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 11:04 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00024s 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
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```



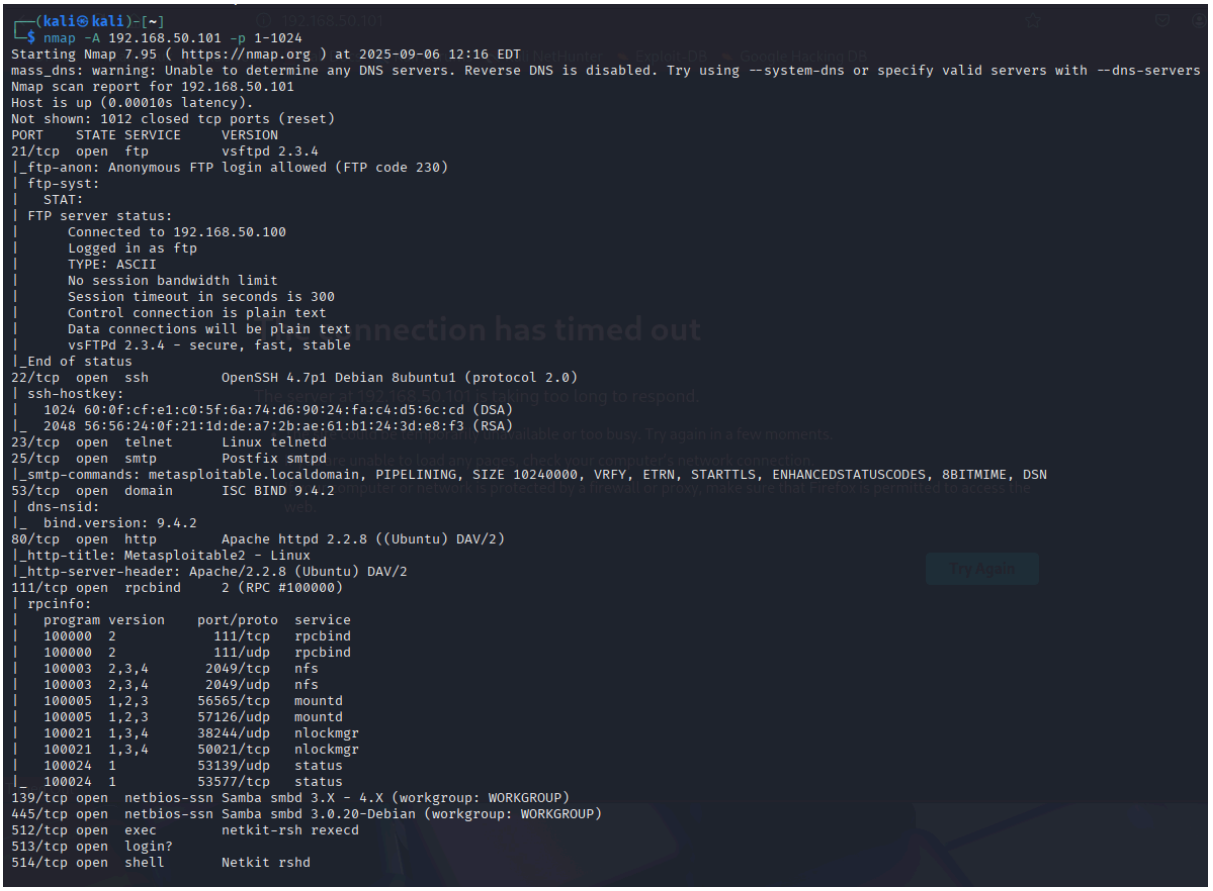
in questi screenshot ho lanciato il comando sT di nmap che è un metodo di scansione più invasivo e come vediamo dalla cattura di wireshark completa tutti i passaggi del 3 way handshake perchè per stabilire se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto deve completare tutti i passaggi del 3 way handshake (esempio sulla porta 80 SYN poi ACK infine RTS,ACK) per le porte chiuse i pacchetti inviati saranno RTS-ACK

scansione SYN sulle porte well-known



in questi screenshot ho lanciato il comando sS di nmap detto anche SYN scan che è un metodo meno invasivo rispetto sT in quanto una volta che ha ricevuto il pacchetto SYN ACK dalla macchina non conclude il 3 way handshake vede solo se la porta è aperta e chiude la comunicazione la cattura con wireshark evidenzia proprio questo comportamento ovvero che il 3 way handshake non viene concluso ma nelle porte aperte viene inviato solo il pacchetto SYN subito dopo l'invio come si vede dallo screen ricevuto il pacchetto SYN ACK la macchina chiude la connessione (esempio sulla porta 80) con il pacchetto RTS, stessa cosa per sT se riceviamo dalla macchina il pacchetto RST-ACK la porta è chiusa.

scansione switch -A sulle porte well known



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 12:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00010s 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 192.168.50.100
|      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
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      56565/tcp   mountd
|   100005  1,2,3      57126/udp   mountd
|   100021  1,3,4      38244/udp   nlockmgr
|   100021  1,3,4      50021/tcp   nlockmgr
|   100024  1          53139/udp   status
|_  100024  1          53577/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (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?
514/tcp open  shell       Netkit rshd
```

```
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:9A:8B:1E (PCS Systemtechnik/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:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-06T14:16:46-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 3h59m58s, deviation: 2h49m42s, median: 1h59m58s

TRACEROUTE
HOP RTT     ADDRESS
1   0.10 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 75.17 seconds
```

la scansione con il comando -A di nmap è quella più invasiva ma ci consente di ottenere più informazioni sulla macchina target, perché attiva l'OS detection ovvero rileva il sistema operativo, version detection ovvero il rilevamento delle versioni dei servizi,script scanning e traceroute per scoprire il percorso dei pacchetti.