

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
```

Capturing from eth0 (tcp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.101	TCP	74	42740 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
2	0.000023370	192.168.50.100	192.168.50.101	TCP	74	50066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
3	0.000050780	192.168.50.100	192.168.50.101	TCP	74	37752 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
4	0.000084200	192.168.50.100	192.168.50.101	TCP	74	50372 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
5	0.000094590	192.168.50.100	192.168.50.101	TCP	74	56168 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
6	0.000110260	192.168.50.101	192.168.50.100	TCP	60	256 → 42740 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.000110410	192.168.50.101	192.168.50.100	TCP	74	80 → 50066 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=451762 TSecr=2873779243 WS=128
8	0.000110450	192.168.50.101	192.168.50.100	TCP	74	25 → 37752 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=451762 TSecr=2873779243 WS=128
9	0.000122870	192.168.50.100	192.168.50.101	TCP	66	50066 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2873779243 TSecr=451762
10	0.000128130	192.168.50.100	192.168.50.101	TCP	66	37752 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2873779243 TSecr=451762
11	0.000153100	192.168.50.101	192.168.50.100	TCP	74	111 → 50372 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=451762 TSecr=2873779243 WS=128
12	0.000153220	192.168.50.101	192.168.50.100	TCP	60	199 → 56168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.000156780	192.168.50.100	192.168.50.101	TCP	66	50372 → 111 [ACK] Seq=0 Ack=1 Win=64256 Len=0 TSval=2873779243 TSecr=451762
14	0.000188140	192.168.50.100	192.168.50.101	TCP	74	59910 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
15	0.000211830	192.168.50.100	192.168.50.101	TCP	74	37806 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
16	0.000234100	192.168.50.101	192.168.50.100	TCP	60	993 → 59910 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	0.000240390	192.168.50.100	192.168.50.101	TCP	74	59926 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
18	0.000253700	192.168.50.101	192.168.50.100	TCP	60	995 → 37806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.000281280	192.168.50.101	192.168.50.100	TCP	60	443 → 59926 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	0.000291450	192.168.50.100	192.168.50.101	TCP	74	52862 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
21	0.000316030	192.168.50.100	192.168.50.101	TCP	74	43680 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2873779243 TSecr=0 WS=128
22	0.000339250	192.168.50.101	192.168.50.100	TCP	74	22 → 52862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=451762 TSecr=2873779243 WS=128
23	0.000341250	192.168.50.100	192.168.50.101	TCP	66	52862 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2873779243 TSecr=451762
24	0.000371240	192.168.50.101	192.168.50.100	TCP	60	135 → 43680 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.000385170	192.168.50.100	192.168.50.101	TCP	66	50066 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2873779243 TSecr=451762

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec 9a:8b:1e (08:00:27:9a:8b:1e)

Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101

Transmission Control Protocol, Src Port: 50066, Dst Port: 80, Seq: 0, Len: 0

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

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101 -p 1-1024
/usr/lib/nmap/nmap: unrecognized option '-1024'
See the output of nmap -h for a summary of options.

(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 11:36 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 (0.000067s 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: 08:00:27:9A:8B:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Capturing from eth0 (tcp)						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.101	TCP	58	38258 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000019880	192.168.50.100	192.168.50.101	TCP	58	38258 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000024750	192.168.50.100	192.168.50.101	TCP	58	38258 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.000028770	192.168.50.100	192.168.50.101	TCP	58	38258 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.000032470	192.168.50.100	192.168.50.101	TCP	58	38258 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.000036690	192.168.50.100	192.168.50.101	TCP	58	38258 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.000040780	192.168.50.100	192.168.50.101	TCP	58	38258 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.000045150	192.168.50.100	192.168.50.101	TCP	58	38258 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.000049400	192.168.50.100	192.168.50.101	TCP	58	38258 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.000054100	192.168.50.100	192.168.50.101	TCP	58	38258 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.000125705	192.168.50.101	192.168.50.100	TCP	60	554 → 38258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.000125865	192.168.50.101	192.168.50.100	TCP	60	995 → 38258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.000125905	192.168.50.101	192.168.50.100	TCP	60	22 → 38258 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
14	0.000125945	192.168.50.101	192.168.50.100	TCP	60	445 → 38258 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
15	0.000125985	192.168.50.101	192.168.50.100	TCP	60	256 → 38258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.000126015	192.168.50.101	192.168.50.100	TCP	60	80 → 38258 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	0.000126055	192.168.50.101	192.168.50.100	TCP	60	23 → 38258 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
18	0.000126085	192.168.50.101	192.168.50.100	TCP	60	199 → 38258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.000146425	192.168.50.100	192.168.50.101	TCP	54	38258 → 22 [RST] Seq=1 Win=0 Len=0
20	0.000152985	192.168.50.100	192.168.50.101	TCP	54	38258 → 445 [RST] Seq=1 Win=0 Len=0
21	0.000156995	192.168.50.100	192.168.50.101	TCP	54	38258 → 80 [RST] Seq=1 Win=0 Len=0
▶ Frame 9: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0 ▶ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_9a:8b:1e (08:00:27:9a:8b:1e) ▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101 ▶ Transmission Control Protocol, Src Port: 38258, Dst Port: 25, Seq: 0, Len: 0						

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-command: 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.

