W9D1 - Pratica (2) - Nmap Scan - Report

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.

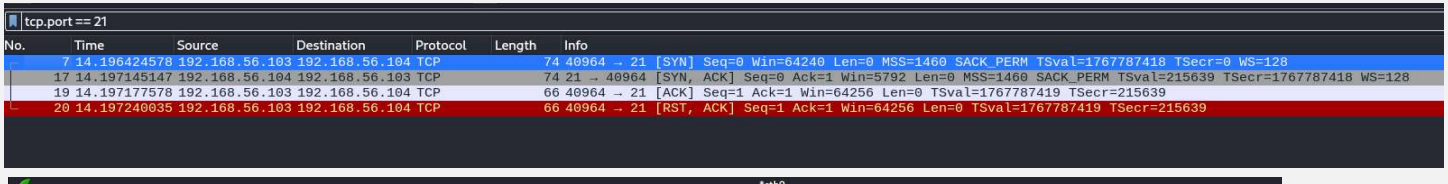
Cybersecurity Analyst

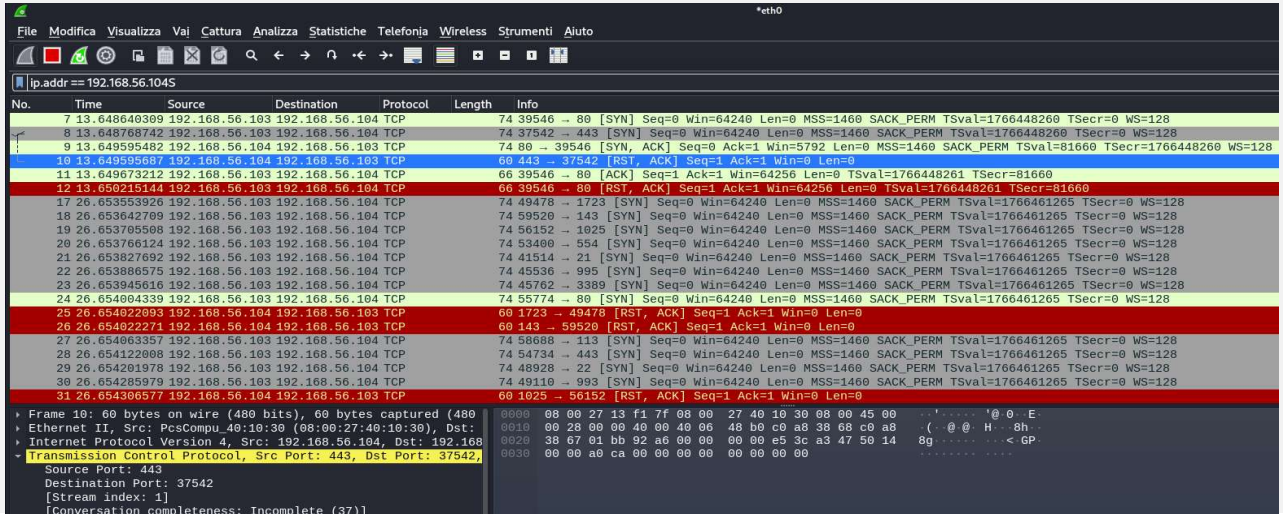
Studente:
Andrea Scarmagnani
Docente:
Giuseppe Placanica

	Nmap scan report for 192.168.56.104
Targhet:	192.168.56.104
Note:	nmap - sT = scansione con 3-way-handshake completa.
	Nella foto sotto si vede l'analisi con wireshark dove le chiamate risultano complete.

Scansione TCP sulle porte well-known

Id	Data	Target	Comando eseguito	Descrizione trovata	N°Porta	Stato_Porta	Servizio	Versione	Descrizione	Vulnerabilità	MEC Address
1	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	21/tcp open ftp	21	OPEN	ftp				No
2	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	22/tcp open ssh	22	OPEN	ssh				No
3	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	23/tcp open telnet	23	OPEN	telne				No
4	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	25/tcp open smtp	25	OPEN	smtp				No
5	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	53/tcp open domain	53	OPEN	domai				No
6	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	80/tcp open http	80	OPEN	http				No
7	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	111/tcp open rpcbind	111	OPEN	rpcbi				No
8	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	139/tcp open netbios-ssn	139	OPEN	netbi				No
9	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	445/tcp open microsoft-ds	445	OPEN	micro				No
10	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	512/tcp open exec	512	OPEN	exec				No
11	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	513/tcp open login	513	OPEN	login				No
12	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	514/tcp open shell	514	OPEN	shell				No
13	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	1099/tcp open rmiregistry	1099	OPEN	rmire				No
14	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	1524/tcp open ingreslock	1524	OPEN	ingre				No
15	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	2049/tcp open nfs	2049	OPEN	nfs				No
16	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	2121/tcp open ccproxy-ftp	2121	OPEN	ccpro				No
17	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	3306/tcp open mysql	3306	OPEN	mysql				No
18	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	5432/tcp open postgresql	5432	OPEN	postg				No
19	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	5900/tcp open vnc	5900	OPEN	vnc				No
20	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	6000/tcp open X11	6000	OPEN	X11				No
21	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	6667/tcp open irc	6667	OPEN	irc				No
22	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	8009/tcp open ajp13	8009	OPEN	ajp13				No
23	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:37 EST	192.168.1.76	└─$ nmap -sT 192.168.56.104	8180/tcp open unknown	8180	OPEN	unkno				No
	Totale						**23**				**23**





```
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 3845956423
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
```

Targhet:	192.168.56.104
Note:	nmap - sS = scansione non completa qui il 3-way-handshake non è completo viene interrotto appena viene data risposta. Nella foto sotto si vede l'analisi con wireshark dove le chiamate risultano interrotte creando meno rumore all'interno della rete

Scansione SYN sulle porte well-known

Colonna1	Data	Target	Comando eseguito	Descrizione trovata	NºPorta	Stato_Porta	Servizio	Versione	Descrizione	Vulnerabilità	MEC Address
1	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	21/tcp open ftp	21	OPEN	ftp				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
2	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	22/tcp open ssh	22	OPEN	ssh				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
3	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	23/tcp open telnet	23	OPEN	telne				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
4	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	25/tcp open smtp	25	OPEN	smtp				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
5	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	53/tcp open domain	53	OPEN	domai				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
6	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	80/tcp open http	80	OPEN	http				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
7	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	111/tcp open rpcbind	111	OPEN	rpcbi				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
8	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	139/tcp open netbios-ssn	139	OPEN	netbi				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
9	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	445/tcp open microsoft-ds	445	OPEN	micro				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
10	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	512/tcp open exec	512	OPEN	exec				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
11	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	513/tcp open login	513	OPEN	login				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
12	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	514/tcp open shell	514	OPEN	shell				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
13	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	1099/tcp open rmiregistry	1099	OPEN	rmire				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
14	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	1524/tcp open ingreslock	1524	OPEN	ingre				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
15	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	2049/tcp open nfs	2049	OPEN	nfs				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
16	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	2121/tcp open ccproxy-ftp	2121	OPEN	ccpro				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
17	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	3306/tcp open mysql	3306	OPEN	mysql				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
18	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	5432/tcp open postgresql	5432	OPEN	postg				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
19	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	5900/tcp open vnc	5900	OPEN	vnc				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
20	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	6000/tcp open X11	6000	OPEN	X11				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
21	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	6667/tcp open irc	6667	OPEN	irc				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
22	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	8009/tcp open ajp13	8009	OPEN	ajp13				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
23	Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:54 EST	192.168.1.76	└─$ sudo nmap -sS 192.168.56.104	8180/tcp open unknown	8180	OPEN	unkno				MAC Address: 08:00:27:40:10:30 (Oracle VirtualBox virtual NIC)
	Totale						**23**				

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
53	24.061017361	192.168.56.103	192.168.56.104	TCP	58	52789 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78	24.062602915	192.168.56.104	192.168.56.103	TCP	60	21 → 52789 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
81	24.062650818	192.168.56.103	192.168.56.104	TCP	54	52789 → 21 [RST] Seq=1 Win=0 Len=0

ip.addr == 192.168.56.104

No.	Time	Source	Destination	Protocol	Length	Info
14	24.058981008	192.168.56.103	192.168.56.104	TCP	58	52789 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	24.059028192	192.168.56.103	192.168.56.104	TCP	58	52789 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	24.059074991	192.168.56.103	192.168.56.104	TCP	58	52789 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	24.059122176	192.168.56.103	192.168.56.104	TCP	58	52789 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	24.059169287	192.168.56.103	192.168.56.104	TCP	58	52789 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	24.059255521	192.168.56.103	192.168.56.104	TCP	58	52789 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	24.059305046	192.168.56.103	192.168.56.104	TCP	58	52789 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	24.059360354	192.168.56.104	192.168.56.103	TCP	60	1025 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	24.059360508	192.168.56.104	192.168.56.103	TCP	60	135 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	24.059603735	192.168.56.104	192.168.56.103	TCP	60	443 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	24.059603851	192.168.56.104	192.168.56.103	TCP	60	554 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	24.059881793	192.168.56.104	192.168.56.103	TCP	60	3306 → 52789 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26	24.059881898	192.168.56.104	192.168.56.103	TCP	60	3389 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	24.059881929	192.168.56.104	192.168.56.103	TCP	60	587 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	24.059881954	192.168.56.104	192.168.56.103	TCP	60	1723 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	24.059881975	192.168.56.104	192.168.56.103	TCP	60	110 → 52789 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	24.059932730	192.168.56.103	192.168.56.104	TCP	54	52789 → 3306 [RST] Seq=1 Win=0 Len=0
31	24.060357321	192.168.56.104	192.168.56.103	TCP	60	53 → 52789 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
32	24.060405375	192.168.56.103	192.168.56.104	TCP	54	52789 → 53 [RST] Seq=1 Win=0 Len=0
33	24.060505932	192.168.56.103	192.168.56.104	TCP	58	52789 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	24.060559212	192.168.56.103	192.168.56.104	TCP	58	52789 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
[Conversation completeness: Incomplete (37)]
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 0
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 791906321
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
```

```
0000  08 00 27 13 f1 7f 08 00  27 40 10 30 08 00 45 00   ··'·····  '@·0··E·
0010  00 28 00 00 40 00 40 06  48 b0 c0 a8 38 68 c0 a8   ·(··@·@·  H···8h··
0020  38 67 0d 3d ce 35 00 00  00 00 2f 33 88 11 50 14   8g·=·5··  ··/3··P·
0030  00 00 2a f9 00 00 00 00  00 00 00 00              ··*·····  ····
```