Esercitazione W9D1-2

Ilaria Pedrelli

Network Scanning con Nmap

Esecuzione di diversi tipi di scan (TCP,SYN, con Switch -A) su porte Well-Known.

1. Scansione con comando -sT (TCP)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 0-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 10:43 EST
Nmap scan report for 192.168.50.101
Host is up (0.00051s latency).
Not shown: 1013 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:D3:7B:60 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.04 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

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

No.	Time	Source	Destination	Protocol	Length	Info
2226	17.888164815	192.168.50.100	192.168.50.101	TCP	74	42304 → 320 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626037 TSecr=0 WS=128
2227	17.888208741	192.168.50.100	192.168.50.101	TCP	74	41520 → 288 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626037 TSecr=0 WS=128
2228	17.888246321	192.168.50.101	192.168.50.100	TCP	60	208 → 51974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2229	17.888246491	192.168.50.101	192.168.50.100	TCP	60	777 → 41404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2230	17.888246541	192.168.50.101	192.168.50.100	TCP	60	971 → 50240 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2231	17.888246571	192.168.50.101	192.168.50.100	TCP	60	660 → 53476 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2232	17.888246591	192.168.50.101	192.168.50.100	TCP	60	597 → 41236 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2233	17.888302105	192.168.50.100	192.168.50.101	TCP	74	39528 → 573 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626037 TSecr=0 WS=128
2234	17.888352637	192.168.50.100	192.168.50.101	TCP	74	45696 → 503 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626037 TSecr=0 WS=128
2235	17.888397083	192.168.50.100	192.168.50.101	TCP	74	39928 → 705 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626037 TSecr=0 WS=128
2236	17.888489113	192.168.50.101	192.168.50.100	TCP	60	738 → 49582 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2237	17.888489253	192.168.50.101	192.168.50.100	TCP	60	320 → 42304 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2238	17.888489273	192.168.50.101	192.168.50.100	TCP	60	288 → 41520 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2239	17.888455152	192.168.50.100	192.168.50.101	TCP	74	50196 → 109 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4138626038 TSecr=0 WS=128
2240	17.888659322	192.168.50.101	192.168.50.100	TCP	60	573 → 39528 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2241	17.888956476	192.168.50.101	192.168.50.100	TCP	60	503 → 45696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2242	17.888956526	192.168.50.101	192.168.50.100	TCP	60	705 → 39928 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2243	17.888956556	192.168.50.101	192.168.50.100	TCP	60	109 → 50196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2244	98.446403667	192.168.50.101	192.168.50.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix …
2245	98.446404109	192.168.50.101	192.168.50.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

Posso innanzitutto notare le porte aperte e con la cattura con Wireshark prendere come esempio la porta 80 e notare come viene concluso il 3-way-handshake, infatti, dopo aver inviato il pacchetto SYN Kali Linux chiude il pacchetto con RST ACK.

2. Scansione con comando -sS (SYN)

In questo caso invece si può notare come non viene chiuso il ciclo 3-way-handshake

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 0-1024
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 11:00 EST
Nmap scan report for 192.168.50.101
Host is up (0.82s latency).
Not shown: 1013 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:D3:7B:60 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.35 seconds
```

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

No.	Time	Source	Destination	Protocol	Length	Info
43	13.087300436	192.168.50.100	192.168.50.101	TCP	54	53087 → 53 [RST] Seq=1 Win=0 Len=0
44	13.087524784	192.168.50.101	192.168.50.100	TCP	60	139 → 53087 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
45	13.087561211	192.168.50.100	192.168.50.101	TCP	54	53087 → 139 [RST] Seq=1 Win=0 Len=0
46	13.087602742	192.168.50.100	192.168.50.101	TCP	58	53087 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	13.087649575	192.168.50.100	192.168.50.101	TCP	58	53087 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	13.087686654	192.168.50.100	192.168.50.101	TCP	58	53087 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	13.087722309	192.168.50.100	192.168.50.101	TCP	58	53087 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50	13.087757383	192.168.50.100	192.168.50.101	TCP	58	53087 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	13.087794122	192.168.50.100	192.168.50.101	TCP	58	53087 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	13.087829547	192.168.50.100	192.168.50.101	TCP	58	53087 → 72 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	13.087909669	192.168.50.101	192.168.50.100	TCP	60	143 → 53087 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	13.087909789	192.168.50.101	192.168.50.100	TCP	60	80 → 53087 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
55	13.087876920	192.168.50.100	192.168.50.101	TCP	58	53087 → 1008 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56	13.087910381	192.168.50.100	192.168.50.101	TCP	54	53087 → 80 [RST] Seq=1 Win=0 Len=0
57	13.087945424	192.168.50.100	192.168.50.101	TCP	58	53087 → 833 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
58	13.087980289	192.168.50.100	192.168.50.101	TCP	58	53087 → 892 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
59	13.088013438	192.168.50.100	192.168.50.101	TCP	58	53087 → 790 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
60	13.088048322	192.168.50.100	192.168.50.101	TCP	58	53087 → 244 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
61	13.088082925	192.168.50.100	192.168.50.101	TCP	58	53087 → 888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
62	13.088125879	192.168.50.101	192.168.50.100	TCP	60	23 → 53087 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

3. Scansione con switch -A

Questo tipo di scansione mi permette di vedere più informazioni essendo una scansione “aggressiva” . Per esempio posso verificare il servizio e la sua versione, informazioni sul sistema operativo e traceroute che mi mostra ogni hop attraverso cui passa ogni pacchetto e ne mostra il tempo impiegato per ogni hop.

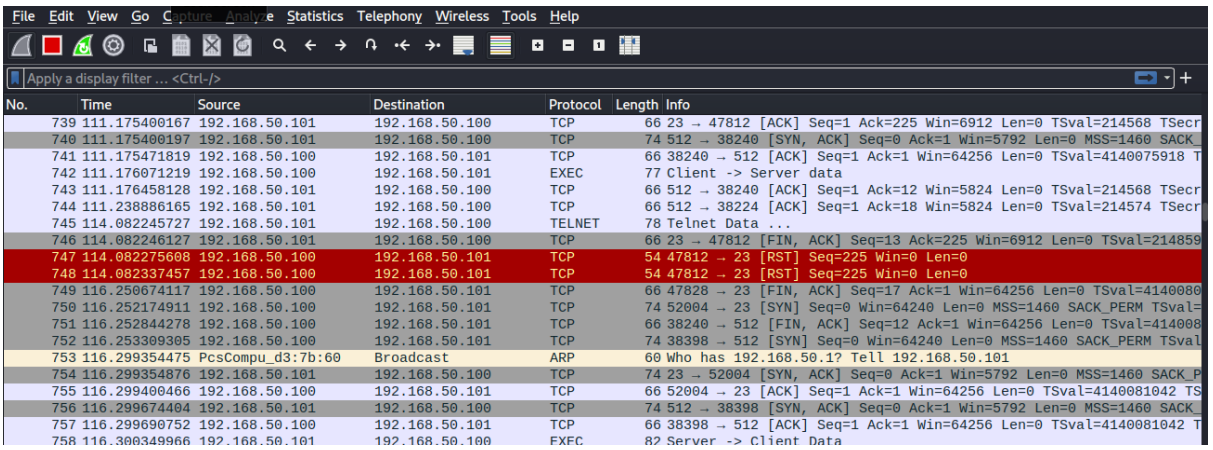
```
File  Actions  Edit  View  Help
┌──$ sudo nmap -A 192.168.50.101 -p 0-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 11:05 EST
Nmap scan report for 192.168.50.101
Host is up (0.12s latency).
Not shown: 1013 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         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?
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      44047/udp   mountd
|   100005  1,2,3      48595/tcp   mountd
|   100021  1,3,4      55405/tcp   nlockmgr
|   100021  1,3,4      57944/udp   nlockmgr
|   100024  1          35760/udp   status
|_  100024  1          37232/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open              Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
```

```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open              Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:D3:7B:60 (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:
|_clock-skew: mean: 2h29m59s, deviation: 3h32m08s, median: -1s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-01-04T11:08:51-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT       ADDRESS
1   123.89 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 248.85 seconds
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
739	111.175400167	192.168.50.101	192.168.50.100	TCP	66	23 → 47812 [ACK] Seq=1 Ack=225 Win=6912 Len=0 TSval=214568 TSecr
740	111.175400197	192.168.50.101	192.168.50.100	TCP	74	512 → 38240 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_
741	111.175471819	192.168.50.100	192.168.50.101	TCP	66	38240 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4140075918 T
742	111.176071219	192.168.50.100	192.168.50.101	EXEC	77	Client -> Server data
743	111.176458128	192.168.50.101	192.168.50.100	TCP	66	512 → 38240 [ACK] Seq=1 Ack=12 Win=5824 Len=0 TSval=214568 TSecr
744	111.238886165	192.168.50.101	192.168.50.100	TCP	66	512 → 38224 [ACK] Seq=1 Ack=18 Win=5824 Len=0 TSval=214574 TSecr
745	114.082245727	192.168.50.101	192.168.50.100	TELNET	78	Telnet Data ...
746	114.082246127	192.168.50.101	192.168.50.100	TCP	66	23 → 47812 [FIN, ACK] Seq=13 Ack=225 Win=6912 Len=0 TSval=214859
747	114.082275608	192.168.50.100	192.168.50.101	TCP	54	47812 → 23 [RST] Seq=225 Win=0 Len=0
748	114.082337457	192.168.50.100	192.168.50.101	TCP	54	47812 → 23 [RST] Seq=225 Win=0 Len=0
749	116.250674117	192.168.50.100	192.168.50.101	TCP	66	47828 → 23 [FIN, ACK] Seq=17 Ack=1 Win=64256 Len=0 TSval=4140080
750	116.252174911	192.168.50.100	192.168.50.101	TCP	74	52004 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
751	116.252844278	192.168.50.100	192.168.50.101	TCP	66	38240 → 512 [FIN, ACK] Seq=12 Ack=1 Win=64256 Len=0 TSval=414008
752	116.253309305	192.168.50.100	192.168.50.101	TCP	74	38398 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval
753	116.299354475	PcsCompu_d3:7b:60	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.101
754	116.299354876	192.168.50.101	192.168.50.100	TCP	74	23 → 52004 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_P
755	116.299400466	192.168.50.100	192.168.50.101	TCP	66	52004 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4140081042 TS
756	116.299674404	192.168.50.101	192.168.50.100	TCP	74	512 → 38398 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_
757	116.299690752	192.168.50.100	192.168.50.101	TCP	66	38398 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4140081042 T
758	116.300349966	192.168.50.101	192.168.50.100	EXEC	82	Server -> Client Data

REPORT							
TCP SCAN							
FONTE		TARGET	SCAN TYPE	SERVIZI ATTIVI			
Indirizzo IP	Range Porte	IP		Port	Stato	Service	
192.168.50.100	0-1024	192.168.50.101	TCP	21	Open	ftp	
192.168.50.100	0-1024	192.168.50.101	TCP	22	Open	ssh	
192.168.50.100	0-1024	192.168.50.101	TCP	23	Open	telnet	
192.168.50.100	0-1024	192.168.50.101	TCP	25	Open	smtp	
192.168.50.100	0-1024	192.168.50.101	TCP	53	Open	domain	
192.168.50.100	0-1024	192.168.50.101	TCP	80	Open	http	
192.168.50.100	0-1024	192.168.50.101	TCP	111	Open	rcpbind	
192.168.50.100	0-1024	192.168.50.101	TCP	139	Open	netbios-ssn	
192.168.50.100	0-1024	192.168.50.101	TCP	445	Open	microsoft-ds	
192.168.50.100	0-1024	192.168.50.101	TCP	512	Open	exec	
192.168.50.100	0-1024	192.168.50.101	TCP	513	Open	login	
192.168.50.100	0-1024	192.168.50.101	TCP	514	Open	shell	
SYN SCAN							
192.168.50.100	0-1024	192.168.50.101	SYN	21	Open	ftp	
192.168.50.100	0-1024	192.168.50.101	SYN	22	Open	ssh	
192.168.50.100	0-1024	192.168.50.101	SYN	23	Open	telnet	
192.168.50.100	0-1024	192.168.50.101	SYN	25	Open	smtp	
192.168.50.100	0-1024	192.168.50.101	SYN	53	Open	domain	
192.168.50.100	0-1024	192.168.50.101	SYN	80	Open	http	
192.168.50.100	0-1024	192.168.50.101	SYN	111	Open	rcpbind	
192.168.50.100	0-1024	192.168.50.101	SYN	139	Open	netbios-ssn	
192.168.50.100	0-1024	192.168.50.101	SYN	445	Open	microsoft-ds	
192.168.50.100	0-1024	192.168.50.101	SYN	512	Open	exec	
192.168.50.100	0-1024	192.168.50.101	SYN	513	Open	login	
192.168.50.100	0-1024	192.168.50.101	SYN	514	Open	shell	