Networking Scanning con NMap

Come richiesto nell'esercizio verranno descritti i vari step richiesti:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 06:20 EST
Nmap scan report for 192.168.50.101
Host is up (0.00065s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:ED:A5:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
```

Qui possiamo vedere la nostra richiesta tramite **nmap -sT** , dove Nmap competa il 3-way-handshake.

SYN -> SYN\ACK -> ACK

No.	Time	Source	Destination	Protocol	Length	Info
29	13.071266672	192.168.50.100	192.168.50.101	TCP	74	55256 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
43	13.071641623	192.168.50.101	192.168.50.100	TCP	74	80 → 55256 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
56	13.071912698	192.168.50.100	192.168.50.101	TCP	66	55256 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=210307696
59	13.071987508	192.168.50.100	192.168.50.101	TCP	66	55256 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2103

	A	B	C	D	E	F	G	H	I
1		Fonte	Destinazio	Protocollo	Porta		Informazioni pacchetti		
2	"192.168.50.100","192.168.50.101","TCP","74","46944 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1424904967 TSecr=0 WS=128"								
3	"192.168.50.101","192.168.50.100","TCP","74","80 > 46944 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=377272 TSecr=1424904967 WS=64"								
4	"192.168.50.100","192.168.50.101","TCP","66","46944 > 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1424904967 TSecr=377272"								
5	"192.168.50.100","192.168.50.101","TCP","66","46944 > 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1424904972 TSecr=377272"								
6									

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 06:04 EST
Nmap scan report for 192.168.50.101
Host is up (0.0056s latency).
Not shown: 977 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
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:ED:A5:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds

┌──(kali㉿kali)-[~]
└─$
```

Qui possiamo notare l'avvio di **nmap -sS** , dove non viene completato il 3-way-handshake e viene chiusa la comunicazione inviando il pacchetto RST (Reset)

SYN -> SYN\ACK -> RST

	Fonte	Destinzione	Protocollo	Porta	Informazioni Pacchetti
3	"192.168.50.100","192.168.50.101","TCP","58","58833 > 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460"				
4	"192.168.50.101","192.168.50.100","TCP","60","80 > 58833 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460"				
5	"192.168.50.100","192.168.50.101","TCP","54","58833 > 80 [RST] Seq=1 Win=0 Len=0"				
6					

```
    62 13.097438311  192.168.50.100  192.168.50.101  TCP  58 36442 → 80 [SYN] Seq=0 Win=1024 L
    75 13.097997504  192.168.50.101  192.168.50.100  TCP  60 80 → 36442 [SYN, ACK] Seq=0 Ack=1
    81 13.098041901  192.168.50.100  192.168.50.101  TCP  54 36442 → 80 [RST] Seq=1 Win=0 Len=
```

dInfine passiamo all'ultimo comando richiesto **nmap -A,** qui verrà effettuato uno scanner più aggressivo, anche il più "rumoroso" a livello di rete rispetto i due precedenti. Qui vengono ricavate molte più informazioni (SO, Versione, script e traceroute)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 07:42 EST
Nmap scan report for 192.168.50.101
Host is up (0.014s latency).
Not shown: 978 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
```

No.	Time	Source	Destination	Protocol	Length	Info
16	13.092247401	192.168.50.100	192.168.50.101	TCP	58	49416 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	13.099887040	192.168.50.101	192.168.50.100	TCP	60	80 → 49416 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29	13.100034114	192.168.50.100	192.168.50.101	TCP	54	49416 → 80 [RST] Seq=1 Win=0 Len=0
2048	13.288284665	192.168.50.100	192.168.50.101	TCP	74	41978 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2103238…
2051	13.288624752	192.168.50.101	192.168.50.100	TCP	74	80 → 41978 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSv…
2052	13.288796705	192.168.50.100	192.168.50.101	TCP	66	41978 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2103238353 TSecr=573728
2137	16.497134487	192.168.50.101	192.168.50.100	TCP	74	[TCP Retransmission] 80 → 41978 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS…
2138	16.497161071	192.168.50.100	192.168.50.101	TCP	66	[TCP Dup ACK 2052#1] 41978 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2…
2145	19.296523098	192.168.50.100	192.168.50.101	HTTP	84	GET / HTTP/1.0
2151	19.302922209	192.168.50.101	192.168.50.100	TCP	66	80 → 41978 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=574329 TSecr=2103244361
2230	19.513087095	192.168.50.101	192.168.50.100	HTTP	1152	HTTP/1.1 200 OK (text/html)
2231	19.513137387	192.168.50.100	192.168.50.101	TCP	66	41978 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=2103244577 TSecr=5…
2232	19.514841984	192.168.50.100	192.168.50.101	TCP	66	41978 → 80 [FIN, ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=2103244579 TS…
2241	19.535002118	192.168.50.101	192.168.50.100	TCP	66	80 → 41978 [FIN, ACK] Seq=1087 Ack=20 Win=5824 Len=0 TSval=574352 TSecr=2…
2242	19.535012082	192.168.50.100	192.168.50.101	TCP	66	41978 → 80 [ACK] Seq=20 Ack=1088 Win=64128 Len=0 TSval=2103244599 TSecr=5…
2887	108.541557073	192.168.50.100	192.168.50.101	TCP	74	32892 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2103333…

	Fonte	Destinazione	Protocollo	Porta	Informazioni pacchetti
2	"192.168.50.101","192.168.50.100","TCP","74","80 > 39206 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=397631 TSecr=1425108436 WS=64"				
3	"192.168.50.100","192.168.50.101","TCP","66","39206 > 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1425108458 TSecr=397631"				
4	"192.168.50.101","192.168.50.100","TCP","74","[TCP Retransmission] 80 > 39206 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=397952 TSecr=1425108458 WS=64"				
5	"192.168.50.100","192.168.50.101","TCP","66","[TCP Dup ACK 2072#1] 39206 > 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1425111664 TSecr=397631"				
6	"192.168.50.100","192.168.50.101","HTTP","84","GET / HTTP/1.0 "				
7	"192.168.50.101","192.168.50.100","TCP","66","80 > 39206 [ACK] Seq=1 Ack=19 Win=5824 Len=0 TSval=398232 TSecr=1425114464"				
8					