ESERCIZIO: Nmap e i suoi comandi

Host discovery
Comando: nmap -sn 192.168.50.101/24

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.50.101/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 18:07 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
MAC Address: 08:00:27:63:87:69 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 28.62 seconds
```

Descrizione: possiamo notare come vengono rilevati 2 host attivi sulla rete

Scansione TCP sulle porte well-know
Comando: nmap -sT -p 1-1023 192.168.50.101

Fonte: 192.168.50.100
Target: 192.168.50.101
Tipo: scansione porte tcp
Risultato: 12 servizi attivi

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
413/tcp	Open	login
514/tcp	Open	shell

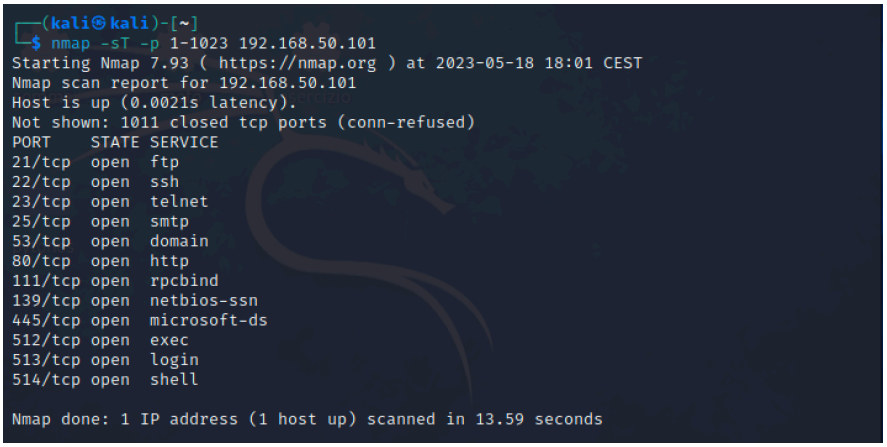
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p 1-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 18:01 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0021s latency).
Not shown: 1011 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

Scansione SYN sulle porte well-know
Comando: nmap -sT -p 1-1023 192.168.50.101

Fonte: 192.168.50.100
Target: 192.168.50.101
Tipo: scansione SYN
Risultato: 12 servizi attivi

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
413/tcp	Open	login
514/tcp	Open	shell



DIFFERENZE

Scansione TCP:

No.	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000000	192.168.50.100	192.168.50.101	TCP	74	59068 → 80 [SYN] Seq=0 Wi
5	0.008319486	192.168.50.101	192.168.50.100	TCP	74	80 → 59068 [SYN, ACK] Seq
7	0.008365668	192.168.50.100	192.168.50.101	TCP	66	59068 → 80 [ACK] Seq=1 Ac

Scansione SYN:

No.	Time	Source	Destination	Protocol	Lengt	Info
19	13.069915439	192.168.50.100	192.168.50.101	TCP	58	51627 → 80 [SYN] Seq=0 Wi
22	13.070952136	192.168.50.101	192.168.50.100	TCP	60	80 → 51627 [SYN, ACK] Seq
23	13.070966080	192.168.50.100	192.168.50.101	TCP	54	51627 → 80 [RST] Seq=1 Wi

Possiamo notare come ci sia differenza tra le due scansioni
Nella prima scansione (TCP) viene completato il 3-way-handshacke creando un canale di comunicazione mentre nella seconda scansione (SYN) non viene completato il 3-way-handshacke e non si crea un canale di comunicazione generando meno ‘rumore’ ma riuscendo in egual modo a recuperare informazioni utili.

SCANSIONE CON SWITCH -A SU PORTE WELL-KNOW

Comando: nmap -p 1-1023 -A 192.168.50.101
Fonte: 192.168.50.100
Target: 192.168.50.101
Risultato: possiamo notare dalla scansione come ci vengono fornite diverse informazioni utili in merito al target come servizi attivi sulle porte e informazioni sul device.