

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

```
(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
```

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 Win=0 Len=0
5	0.008319486	192.168.50.101	192.168.50.100	TCP	74	80 → 59068 [SYN, ACK] Seq=1 Win=0 Len=0
7	0.008365668	192.168.50.100	192.168.50.101	TCP	66	59068 → 80 [ACK] Seq=1 Win=0 Len=0

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 Win=0 Len=0
22	13.070952136	192.168.50.101	192.168.50.100	TCP	60	80 → 51627 [SYN, ACK] Seq=1 Win=0 Len=0
23	13.070966080	192.168.50.100	192.168.50.101	TCP	54	51627 → 80 [RST] Seq=1 Win=0 Len=0

Possiamo notare come ci sia differenza tra le due scansioni

Nella prima scansione (TCP) viene completato il 3-way-handshake creando un canale di comunicazione mentre nella seconda scansione (SYN) non viene completato il 3-way-handshake 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.

```
(kali@kali)-[~]
$ sudo nmap -p 1-1023 -A 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 16:39 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 1011 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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ _smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, S
TARTTLS, 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      43782/udp  mountd
|_   100005  1,2,3      46218/tcp  mountd
|_   100021  1,3,4      47068/tcp  nlockmgr
|_   100021  1,3,4      52894/udp  nlockmgr
|_   100024  1          37202/udp  status
|_   100024  1          40435/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
MAC Address: 08:00:27:63:87:69 (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)
|_ _smb2_time: Protocol negotiation failed (SMB2)
|_ _nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000
000000 (Xerox)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.20-Debian)
|_   Computer name: metasploitable
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: metasploitable.localdomain
|_   System time: 2023-05-18T10:13:33-04:00
|_ _clock-skew: mean: 1h33m01s, deviation: 2h49m43s, median: -26m59s
TRACEROUTE
HOP RTT ADDRESS
1 1.35 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 104.65 seconds
(kali@kali)-[~]
$
```