

# Esercizio nmap

## -Host discovery

Settando le due macchine virtuali (kali e metasploitable) su rete interna con relativi indirizzi ip: 192.168.50.100 e 192.168.50.101 , vado a fare un host discovery sulla rete 192.168.50.0/24 con nmap, usando il comando : nmap -sn 192.168.50.0/24 . Nmap riconosce 2 host, le macchine precedentemente settate.

```
(kali@kali)~$ nmap -sn 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:17 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00028s latency).
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 20.12 seconds
```

## -Scansione TCP sulle porte well-known

Con il comando: nmap -sT -p 0-1023 192.168.50.101, vado a fare una scansione tcp sulle porte well-known. Di seguito il report della scansione.

**Fonte scan:** 192.168.50.100

**Target scan:** 192.168.50.101

**Tipo di scan:** -sT (TCP SCAN) sulle porte 0-1023

**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
513/tcp	open	login
515/tcp	open	shell

```
(kali@kali)~$ nmap -sT -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 08:30 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0015s latency).
Not shown: 1012 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 13.51 seconds
```

## -Scansione SYN sulle porte well-known

Con il comando: `nmap -sS -p 0-1023 192.168.50.101`, vado a fare una scansione Syn sulle porte well-known.  
Di seguito il report della scansione.

**Fonte scan:** 192.168.50.100

**Target scan:** 192.168.50.101

**Tipo di scan:** -sS (SYN SCAN) sulle porte 0-1023

**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
513/tcp	open	login
514/tcp	open	shell

```
(root@kali)-[/home/kali]
# nmap -sS -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:11 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.101
Host is up (0.00049s latency).
Not shown: 1012 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: 08:00:27:0A:28:78 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
```

## -Scansione con switch <<-A>> sulle porte well-known

Con il comando: `nmap -a -p 0-1023 192.168.50.101`, vado a fare una scansione approfondita sulle porte well-known. Di seguito il report della scansione.

**Fonte scan:** 192.168.50.100

**Target scan:** 192.168.50.101

**Tipo di scan:** -A sulle porte 0-1023

**Risultato:** 12 servizi attivi

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Vstpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	Netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	Netbios-ssn	amba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	Login?	
514/tcp	open	shell	Netkit rshd

**Altre info riportate nella scansione:**

**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)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (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: 2023-05-18T09:25:35-04:00

|\_smb2-time: Protocol negotiation failed (SMB2)

|\_clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s

## TRACEROUTE

HOP RTT ADDRESS

1 0.92 ms 192.168.50.101

```
(root@kali) - [/home/kali]
# nmap -A -p 0-1023 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00092s latency).
Not shown: 1012 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-command: 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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
```

```

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      41533/tcp mountd
|_ 100005 1,2,3      47963/udp mountd
|_ 100021 1,3,4      55670/udp nlockmgr
|_ 100021 1,3,4      58679/tcp nlockmgr
|_ 100024 1          36211/udp status
|_ 100024 1          58430/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?      Netkit rshd
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:0A:28:78 (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)
|_ _nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (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: 2023-05-18T09:25:35-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ _clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1 0.92 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 90.10 seconds

```

## Differenze tra scansione completa TCP e SYN

Con l'utilizzo di Wireshark vado ad intercettare le richieste inviate dalla macchina sorgente. Con la scansione completa TCP, notiamo che si va a creare il canale di comunicazione completo del three-way handshake. Nella foto che segue sono andato a filtrare una specifica porta, in questo caso porta 80, per andare a vedere come avviene la comunicazione SYN, SYN-ACK e ACK.

No.	Time	Source	Destination	Protocol	Length	Info
3	13.060239566	192.168.50.100	192.168.50.101	TCP	74	55670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1701108059 TSecr=0 WS=128
5	13.062038808	192.168.50.101	192.168.50.100	TCP	74	80 → 55670 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=718513 TSecr=1701108059 WS=64
6	13.062424187	192.168.50.100	192.168.50.101	TCP	66	55670 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1701108061 TSecr=718513

Invece con la scansione SYN, la comunicazione non si completa e il three-way handshake non viene portato a termine. Infatti come si vede nella prossima foto, lo scambio avviene con SYN, SYN ACK e RST, interrompendo la connessione con RST.

No.	Time	Source	Destination	Protocol	Length	Info
33	13.309657396	192.168.50.100	192.168.50.101	TCP	58	53996 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	13.310016253	192.168.50.101	192.168.50.100	TCP	60	80 → 53996 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
37	13.310025747	192.168.50.100	192.168.50.101	TCP	54	53996 → 80 [RST] Seq=1 Win=0 Len=0

La differenza sta nel fatto che nella scansione TCP si crea il canale di comunicazione, mentre col SYN si interrompe poco prima di crearla, non concludendo il three-way handshake.