Tool Kali Linux Nmap

Dopo aver fatto il ping con Metaspoitable eseguo nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.13.150 -p 1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 01:15 CET
Nmap scan report for 192.168.13.150
Host is up (0.00064s 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
MAC Address: 08:00:27:99:07:5C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

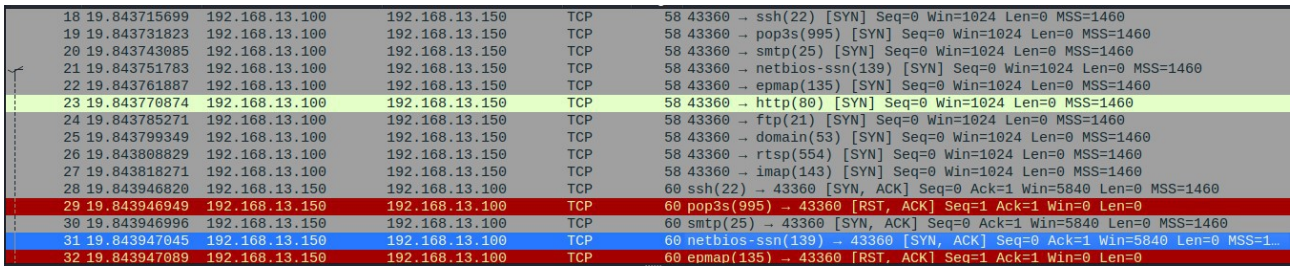
Con wireshark verifico che completi il 3-way-handshake

13	0.070051589	192.168.13.150	192.168.13.100	TCP	74 netbios-ssn(139) → 34884 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1…
14	0.070060245	192.168.13.100	192.168.13.150	TCP	74 52766 → smtp(25) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva…
15	0.070089691	192.168.13.100	192.168.13.150	TCP	66 34884 → netbios-ssn(139) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=164…
16	0.070136664	192.168.13.150	192.168.13.100	TCP	60 epmap(135) → 54142 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	0.070138995	192.168.13.100	192.168.13.150	TCP	74 38324 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSva…
18	0.070136788	192.168.13.150	192.168.13.100	TCP	74 sunrpc(111) → 58788 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 S…
19	0.070156205	192.168.13.100	192.168.13.150	TCP	66 58788 → sunrpc(111) [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=16492448…
20	0.070169973	192.168.13.100	192.168.13.150	TCP	66 34884 → netbios-ssn(139) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva…
21	0.070205018	192.168.13.100	192.168.13.150	TCP	66 58788 → sunrpc(111) [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=164…
22	0.070225624	192.168.13.150	192.168.13.100	TCP	60 pop3s(995) → 57034 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.070225835	192.168.13.150	192.168.13.100	TCP	60 rap(256) → 52096 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	0.070252552	192.168.13.100	192.168.13.150	TCP	74 51138 → telnet(23) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS…
25	0.070293080	192.168.13.100	192.168.13.150	TCP	74 43488 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS…
26	0.070304060	192.168.13.150	192.168.13.100	TCP	60 rtsp(554) → 45144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.070304162	192.168.13.150	192.168.13.100	TCP	60 imap(143) → 45904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Con la scansione nmap -sS invece non dovrebbe completare il 3-way-handshake

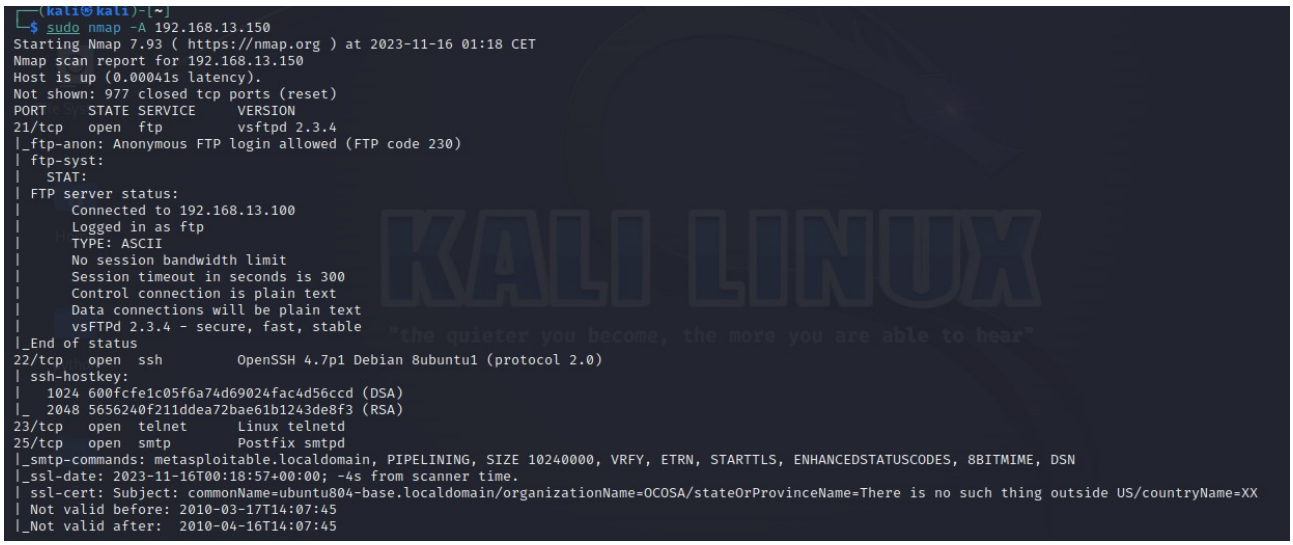
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.13.150 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 01:07 CET
Nmap scan report for 192.168.13.150
Host is up (0.00025s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
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: 08:00:27:99:07:5C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Verifico con wireshark



18	19.843715699	192.168.13.100	192.168.13.150	TCP	58 43360 → ssh(22) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	19.843731823	192.168.13.100	192.168.13.150	TCP	58 43360 → pop3s(995) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	19.843743085	192.168.13.100	192.168.13.150	TCP	58 43360 → smtp(25) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	19.843751783	192.168.13.100	192.168.13.150	TCP	58 43360 → netbios-ssn(139) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	19.843761887	192.168.13.100	192.168.13.150	TCP	58 43360 → epmap(135) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	19.843770874	192.168.13.100	192.168.13.150	TCP	58 43360 → http(80) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	19.843785271	192.168.13.100	192.168.13.150	TCP	58 43360 → ftp(21) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	19.843799349	192.168.13.100	192.168.13.150	TCP	58 43360 → domain(53) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	19.843808829	192.168.13.100	192.168.13.150	TCP	58 43360 → rtsp(554) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	19.843818271	192.168.13.100	192.168.13.150	TCP	58 43360 → imap(143) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	19.843946820	192.168.13.150	192.168.13.100	TCP	60 ssh(22) → 43360 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29	19.843946949	192.168.13.150	192.168.13.100	TCP	60 pop3s(995) → 43360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	19.843946996	192.168.13.150	192.168.13.100	TCP	60 smtp(25) → 43360 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
31	19.843947045	192.168.13.150	192.168.13.100	TCP	60 netbios-ssn(139) → 43360 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1…
32	19.843947089	192.168.13.150	192.168.13.100	TCP	60 epmap(135) → 43360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Scansione con -A dove trovo tutte le info relative al target



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.13.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 01:18 CET
Nmap scan report for 192.168.13.150
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.13.100
|      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
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, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-11-16T00:18:57+00:00; -4s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```