

# NETWORK SCANNING CON NMAP

Nell'esercizio di oggi siamo andati a scansionare la macchina metasploitable con il tool nmap. Abbiamo eseguito diversi tipi di scan:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well known
- Scansione con switch "-A" sulle porte well-known

Abbiamo trovato le porte well-known aperte sul nostro terminale Kali, cioè tra quelle che vanno dalla porta 0 alla 1023:

PORTE	STATE	SERVICE
21	Open	ftp
22	Open	ssh
23	Open	telnet
25	Open	smtp
53	Open	domain
80	Open	http
111	Open	rpcbind
139	Open	netbios-ssn
445	Open	microsoft-ds
512	Open	exec
513	Open	login
514	Open	shell

Tab1

Durante la scansione abbiamo aperto Wireshark intercettando le richieste inviate dalla macchina sorgente.

The screenshot displays a Kali Linux terminal window on the right and a Wireshark network traffic capture on the left. The terminal window shows the command `nmap 192.168.32.101 -T` and its output, which lists open ports and services. The Wireshark interface shows the captured network traffic, with packets 10, 12, and 13 highlighted. Red arrows point from the terminal output to the corresponding packets in Wireshark.

Terminal Output:

```
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -f -g 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

[kali@kali:~]$ nmap 192.168.32.101 -T
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:18 EST
Nmap scan report for 192.168.32.101
Host is up (0.0003s latency).
Not shown: 927 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
1899/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
2386/tcp  open  mysql
5432/tcp  open  postgresql
5908/tcp  open  vnc
6000/tcp  open  xcp
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

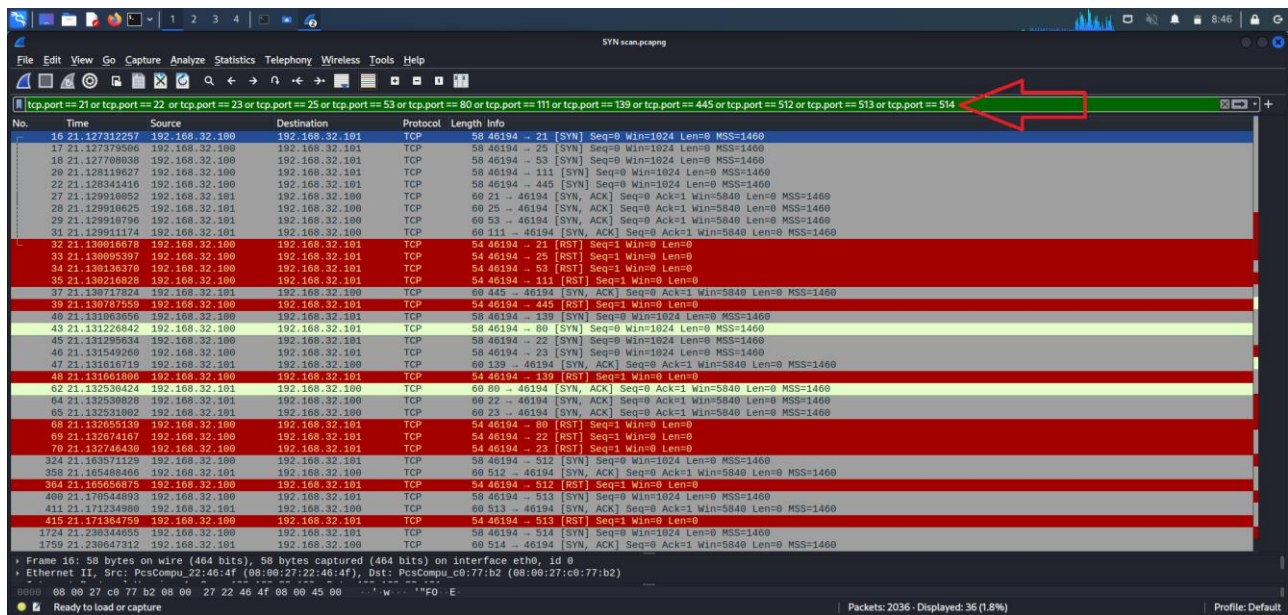
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds

[kali@kali:~]$
```

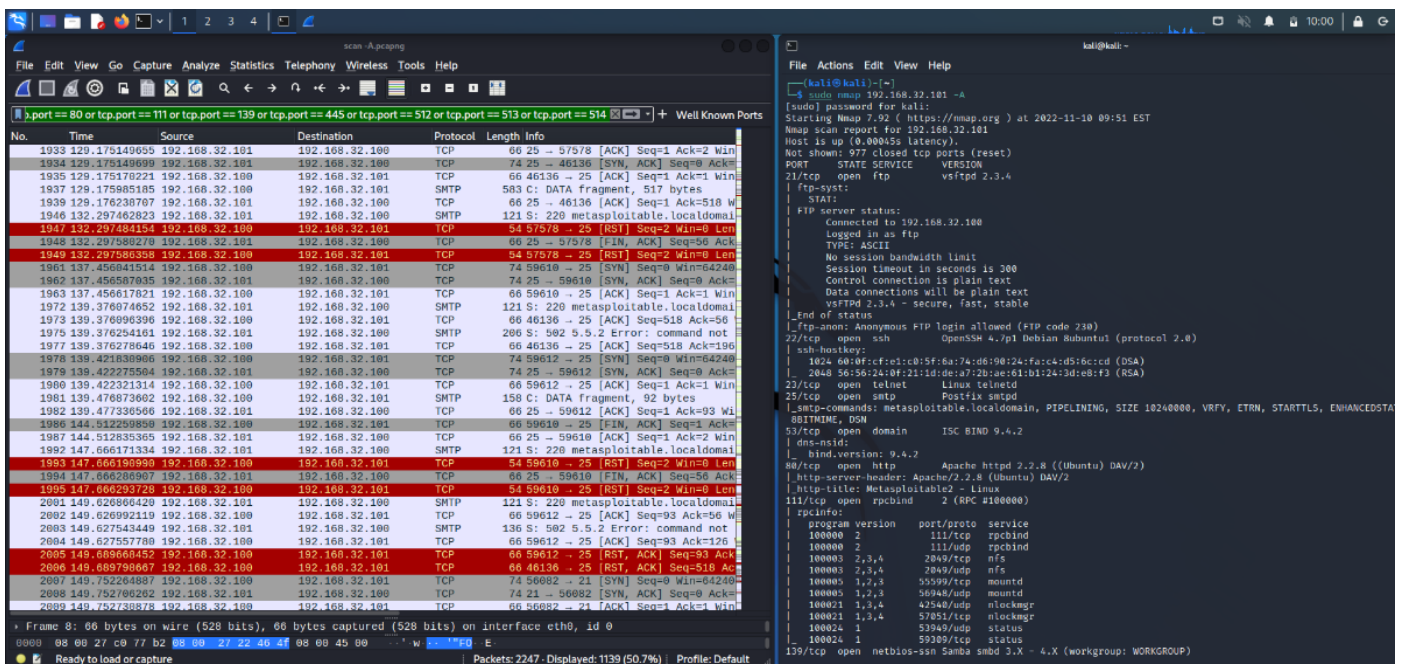
Wireshark Capture:

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu\_22:46:4f (08:00:27:22:46:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
...  
0000 ff ff ff ff ff ff 08 00 27 22 46 4f 08 00 ff ff ff ff ff ff  
Packets: 2056 - Displayed: 2056 (100.0%) | Profile: Default

Abbiamo filtrato per vedere solo le porte interessate (Tab1):



Fatte le ricerche per nmap "IP" -sT e per nmap "IP" -sS abbiamo fatto una scansione -A:



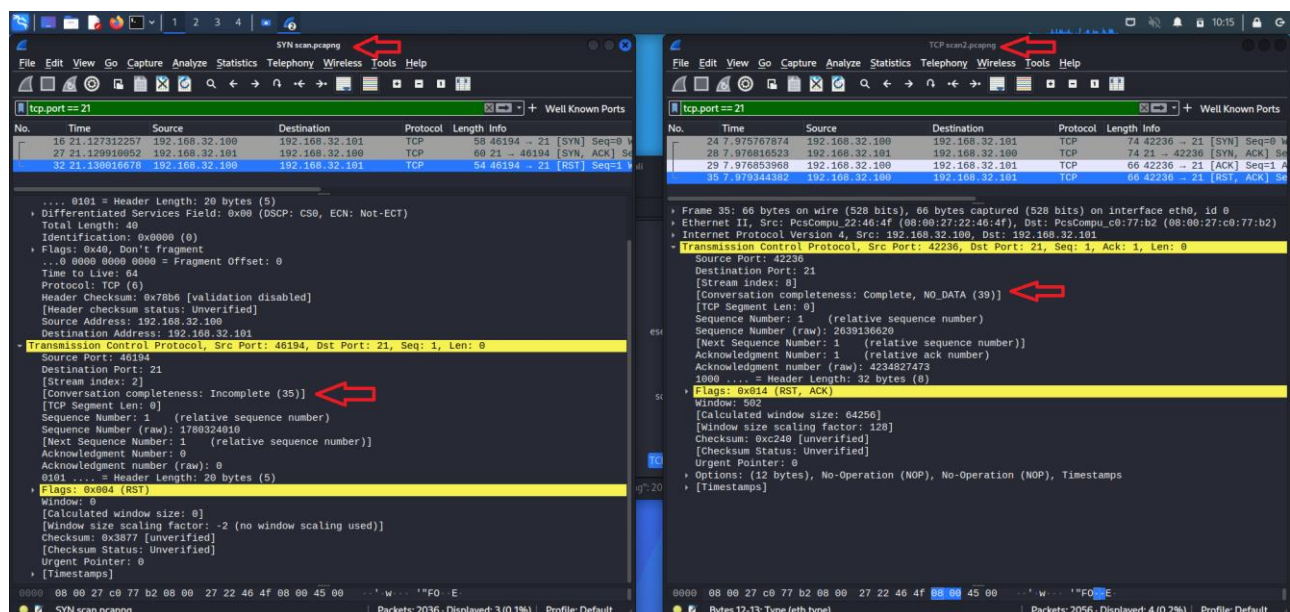
Come possiamo vedere la scansione -A fa una scansione molto più approfondita (img sopra e sotto).

```
kali@kali: ~  
$ sudo nmap 192.168.32.101 -A  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:56 EST  
Nmap scan report for 192.168.32.101  
Host is up (0.0013s 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 192.168.32.100  
|    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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp    open  telnet        Linux telnetd  
25/tcp    open  smtp          Postfix smtpd  
|_smtp-command: metaspoitable.localdomain, PIPELINING, SIZE 1024000, 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 55599/tcp mountd  
| 100005 1,2,3 56948/udp mountd  
| 100021 1,3,4 42540/udp nlockmgr  
| 100021 1,3,4 57051/tcp nlockmgr  
| 100024 1 53949/udp status  
| 100024 1 59309/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)
```

Abbiamo poi evidenziato le porte well-known filtrando le scansioni di Wireshark per notare le differenze:

Qui vediamo un esempio di scansione della stessa porta (porta 21) dove possiamo vedere come la scansione -sT, essendo più invasiva rispetto alla -sS, completa la connessione 3-way-handshake.

Infatti, la scansione TCP darà la connessione completa, mentre, la scansione SYN darà connessione incompleta, dato che verrà chiusa dopo il SYN/ACK.



FONTE SCAN	TARGET SCAN	TIPO DI SCAN	RISULTATO OTTENUTO
192.168.32.100	192.168.32.101	nmap -sT	23 servizi aperte di cui 12 di porte well-known

192.168.32.100	192.168.32.101	nmap -sS	23 servizi aperte di cui 12 di porte well-known
----------------	----------------	----------	--