

NETWORK SCANNING CON NMAP

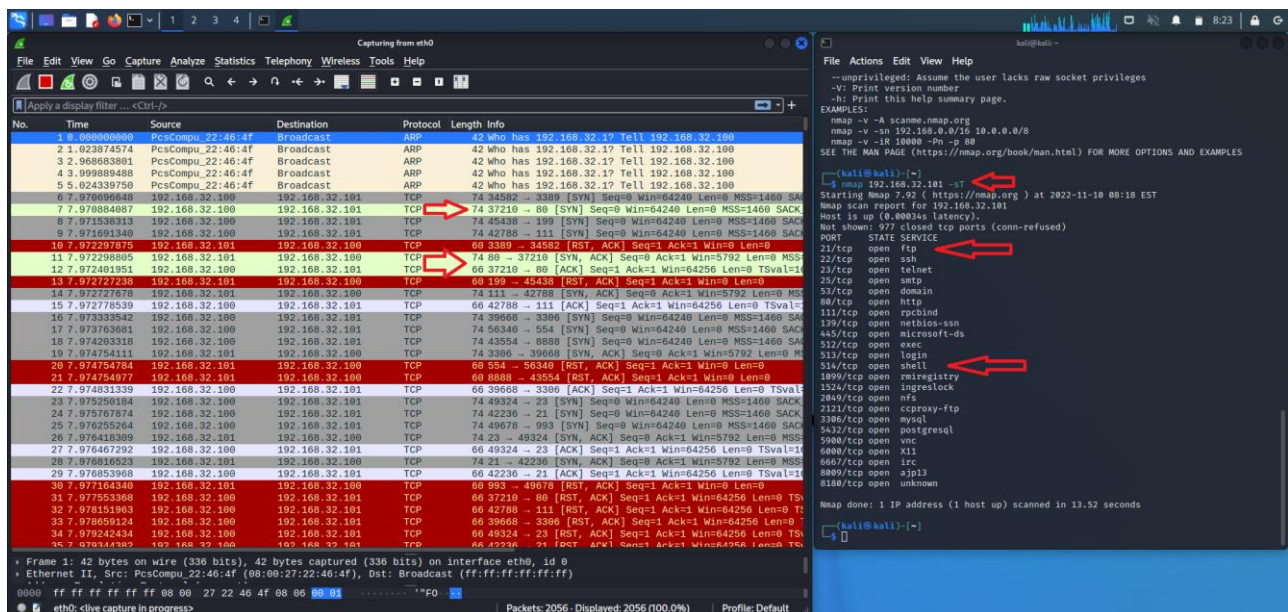
Nell'esercizio di oggi siamo andati a scansionare la macchina metasploitable con il tool nmap. Abbiamo eseguito diversi tipi di scan:

- 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

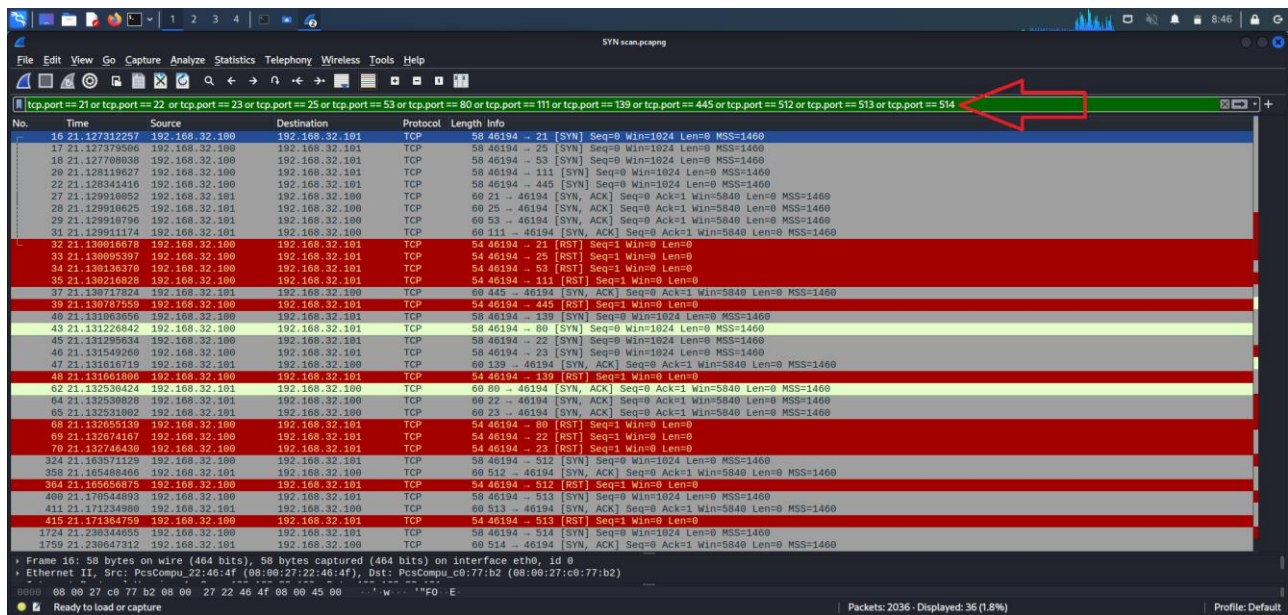
PORT	STATE	SERVICE
21	Open	ftp
22	Open	ssh
23	Open	telnet
25	Open	smtp
53	Open	domain
80	Open	http
111	Open	rpcbind
139	Open	netbios-ssn
445	Open	microsoft-ds
512	Open	exec
513	Open	login
514	Open	shell

Tab1

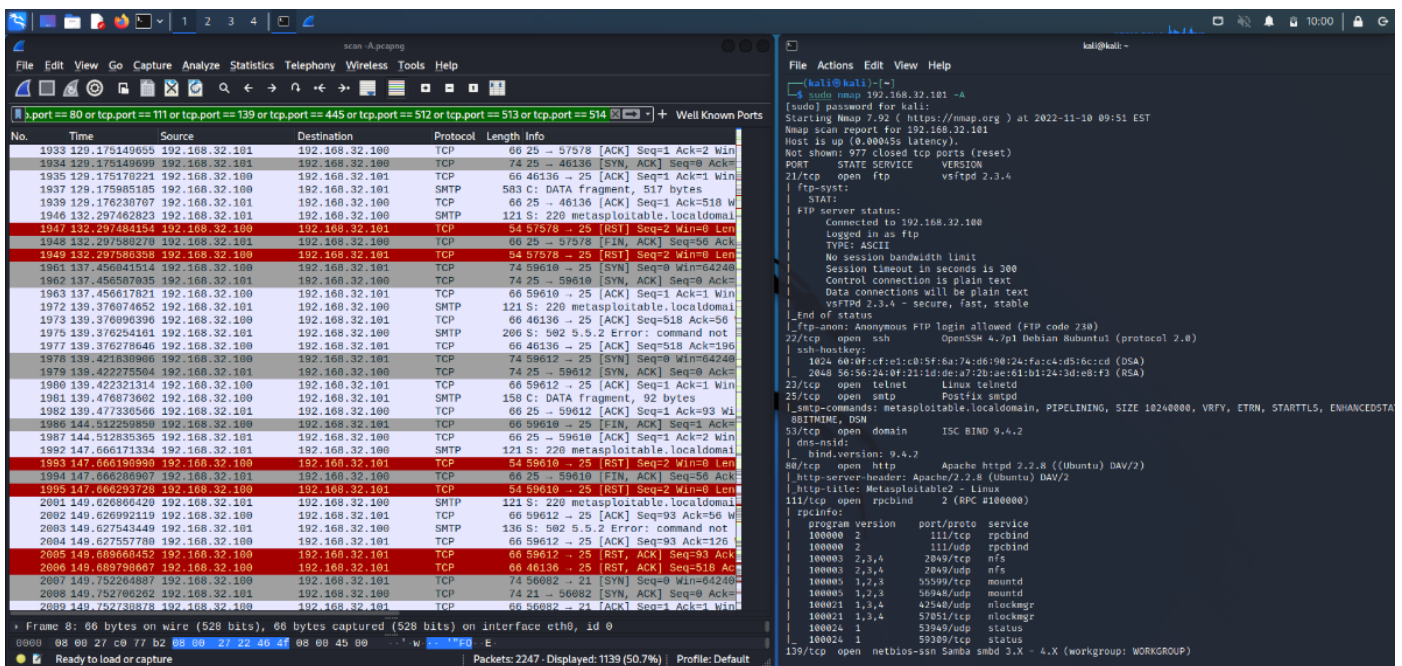


Durante la scansione abbiamo aperto Wireshark intercettando le richieste inviate dalla macchina sorgente.

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:



```

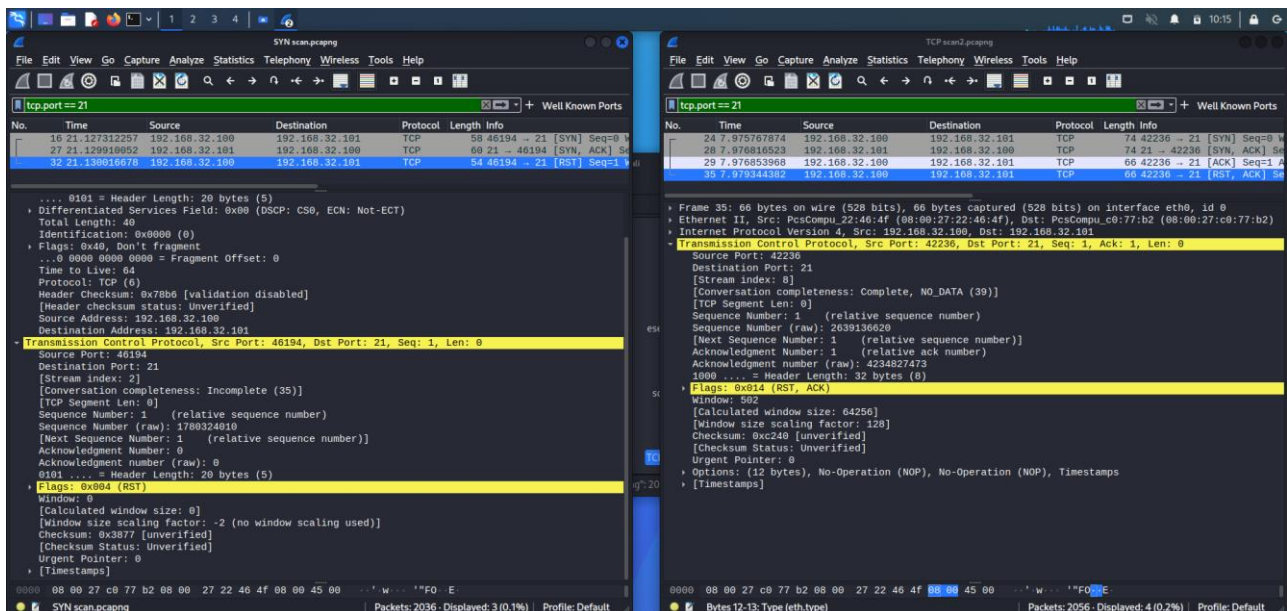
kali@kali: ~
File Actions Edit View Help

(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 scan.
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 nelle 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:



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