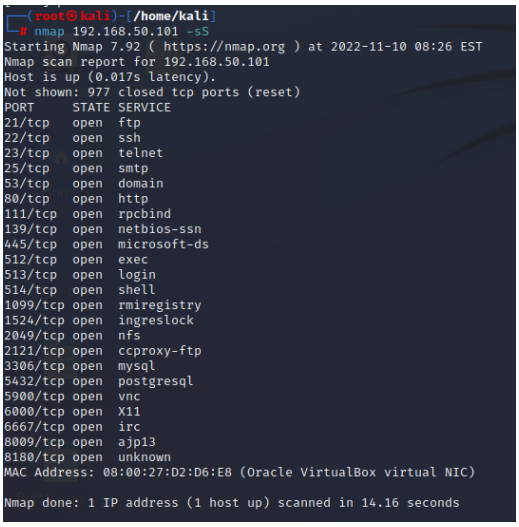
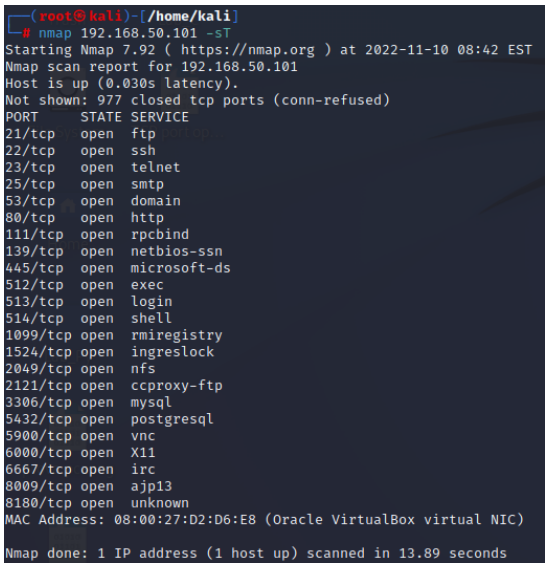
La traccia di oggi ci chiedeva di prendere un po' di confidenza con i comandi di nmap nello specifico:

- Una scansione TCP sulle porte well-known, la quale verrà fatta con con il comando **sudo nmap -sS.** La quale è una scansione molto leggere che non include il 3-way-handshake,in quanto una volta ricevuto il pacchetto SYN/ACK chiude la comunicazione.




- Una scansione SYN sulle porte well-known, la quale verrà fatta con il comando **sudo nmap -sT.** Questa scansione è più aggressiva della precedente in quanto svolge tutti i passaggi del 3-way-handshake creando quindi un canale

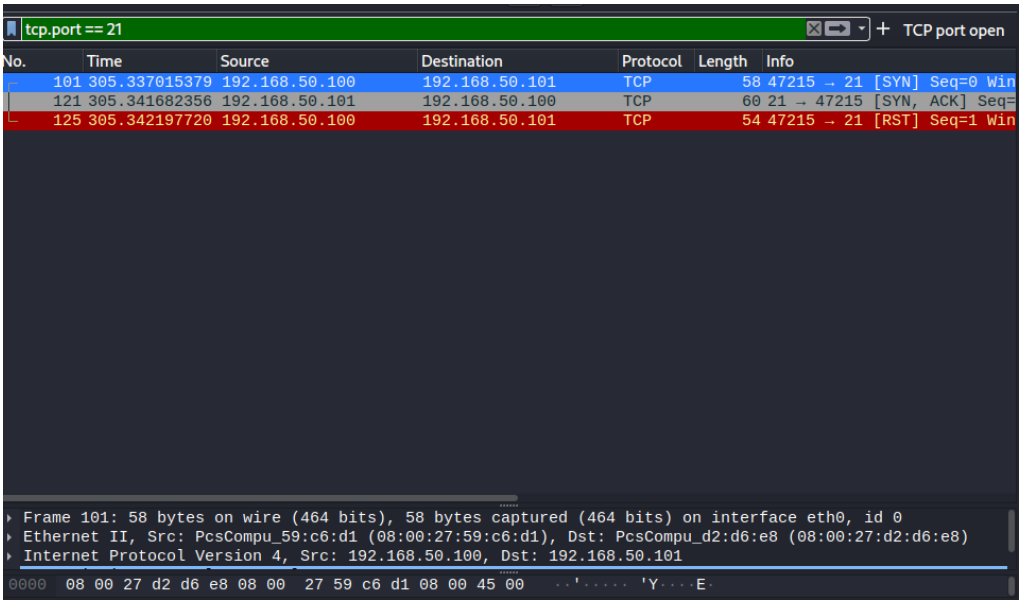


- Una scansione con “-A” sulle porte well-known, la quale verrà fatta con il comando **sudo nmap -A,** questa scansione è la più invadente delle tre questa però ci dara molte più informazioni rispetto alle precedenti due, a discapito di tempo e discrezione**.**

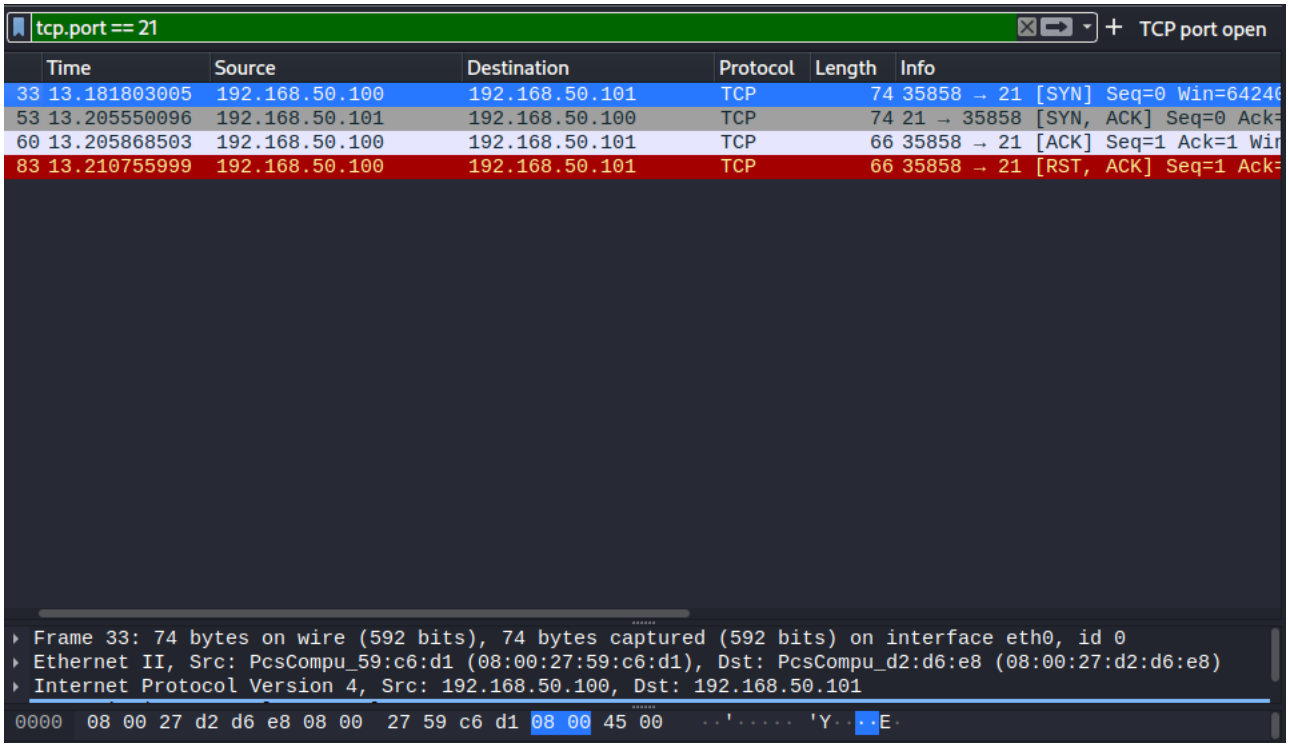
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.50.101 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 08:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| 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 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?
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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
```

## 2) Ora vediamo cosa abbiamo registrato con wireshark

- Questa e la prima scansione con -sS, come possiamo vedere in questo caso il client una volta appurato che la conessione si possibile interrompe la conessione senza creare un canale con il 3-handshake.



- Questa è invece la scansione con -sT, come si può vedere in questo caso il cliente crea un vero e proprio canale con il 3-handshake, inviando prima il segnale SYN , ricevendo poi dal server SYN,ACK, inviando a sua volta l'ACK e chiude la connessione.




Infine questa è la tabellazione come richiesto dalla traccia con la fonte dello scan, il ricevente dello scan, il tipo di scan e i servizi ottenuti.

| INDIRIZZO SRC | INDIRIZZO DSC | SCAN | SERVIZI |
|---|---|---|---|
| 192.168.50.100 (linux) | 192.168.50.101 (meta) | Nmap –sT | 23 - 12 (well Know) |
| 192.168.50.100 (linux) | 192.168.50.101 (meta) | Nmap -sS | 23 - 12 (well Know) |
| 192.168.50.100 (linux) | 192.168.50.101 (meta) | Nmap -A | 23 - 12 (well Know) |