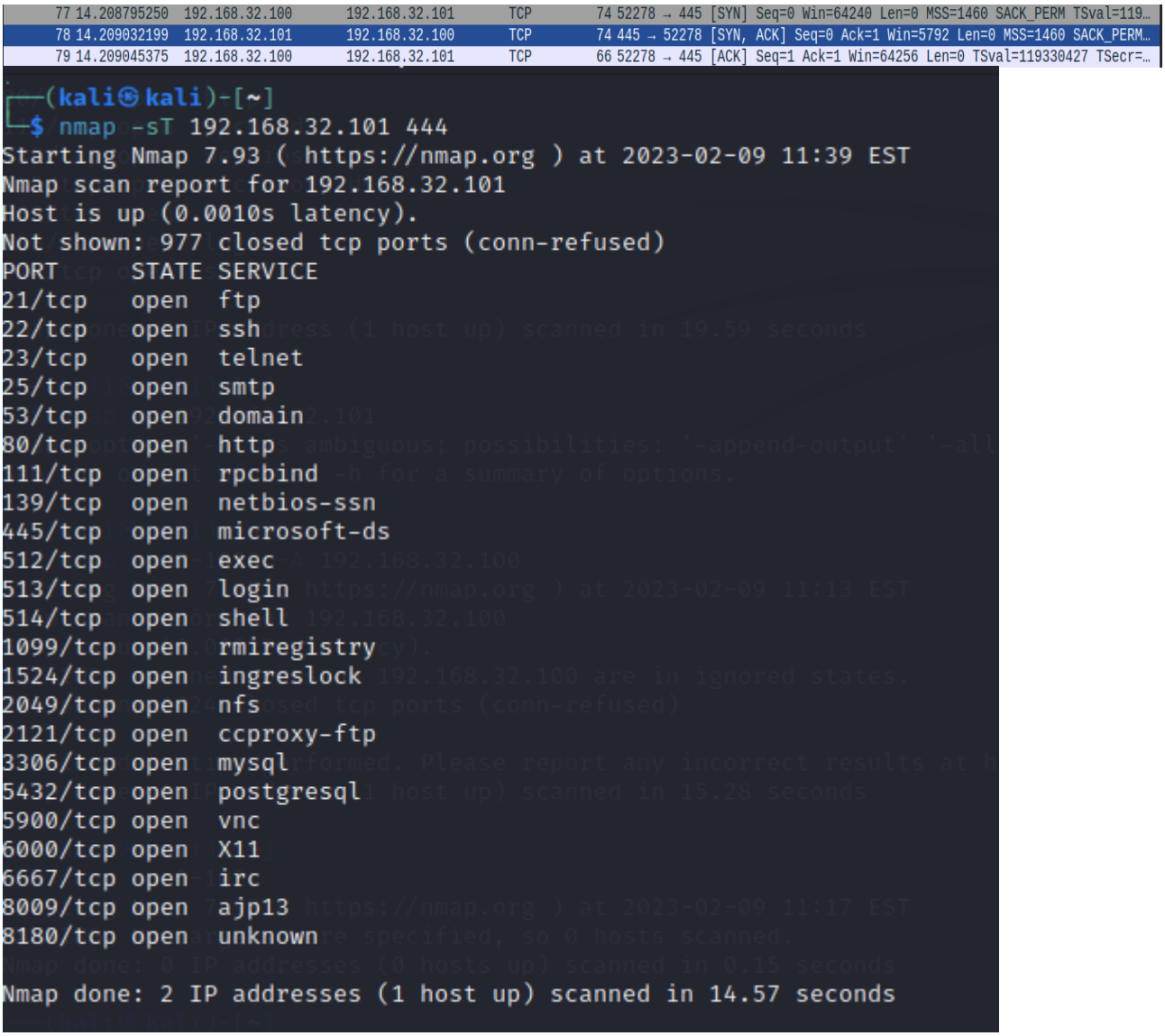
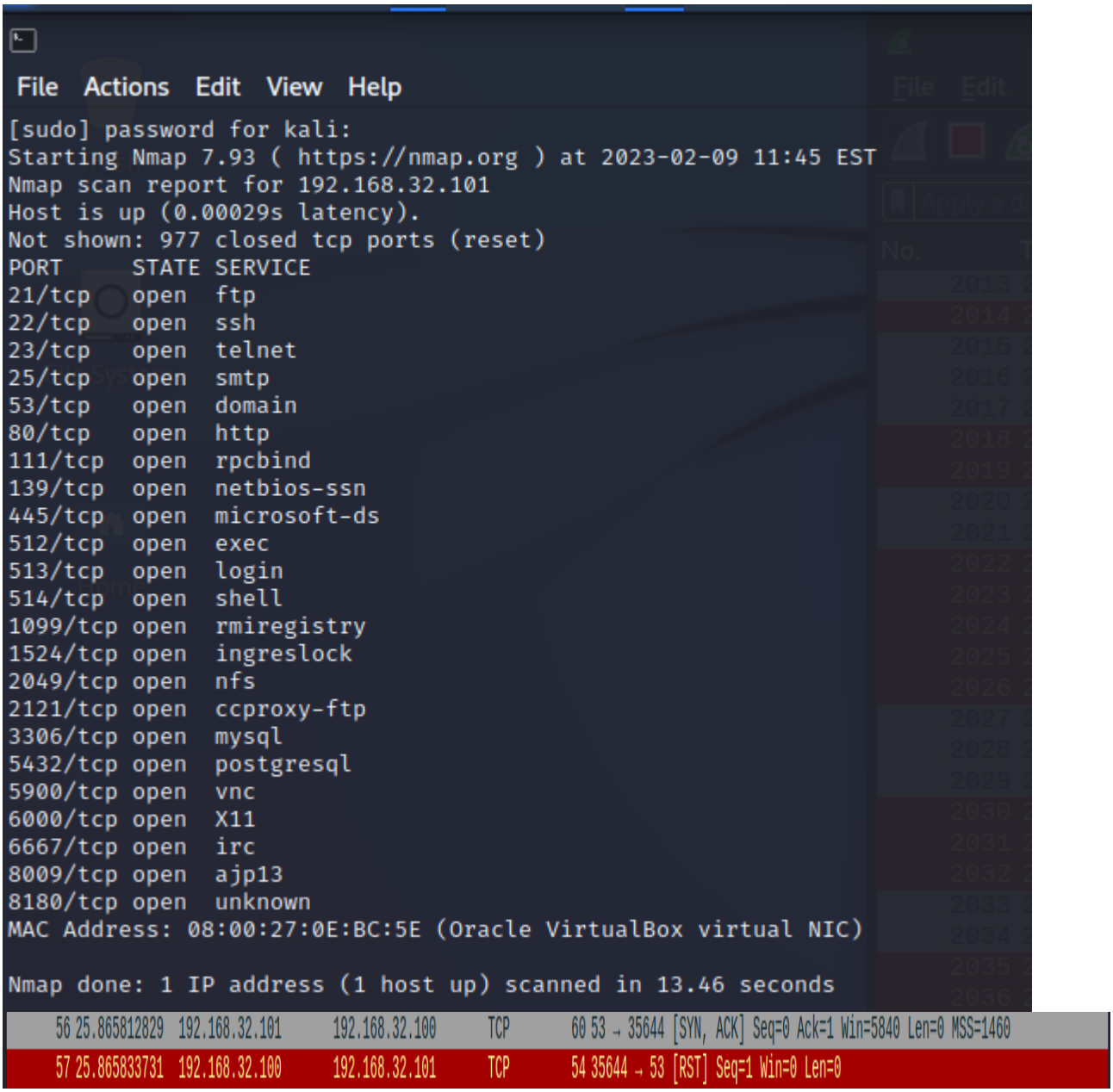
Scansione tcp sulle porte well known:



Come possiamo vedere, utilizzando il comando nmap –sT si scansionano le porte aperte sul server metasploitable con ip indicato, e si scansionera in maniera piu invasiva, terminando il 3 hand shake, dove all inizio (fra la porta 445 e 52278) precisamente kali linux (in questo caso sorgente:192.168.32.100) mandera seq=o a metasploitable(in questo caso destinatario 192.168.32.101), esso rispondera con seq=0 e ack=1 ed a sua volta linux aggiungera valore 1 e rispondera seq=1 e ack=1 terminando il 3 handshake.

Sacansione SYN:



IN Questo caso con il comando nmap –sS abbiamo avviato una scansione meno invasiva evitando di terminare il 3 hand shake: difatti come si puo vedere, le due macchine si rimandano il valore un'unica volta senza terminarlo.

Scansione con switch-a:

```
┌──(kali㉿kali)-[~]
└─$ nmap st 192.168.32.101 -p1-1024
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-09 11:11 EST
Failed to resolve "st".
Nmap scan report for 192.168.32.101
Host is up (0.0014s 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 19.59 seconds
```