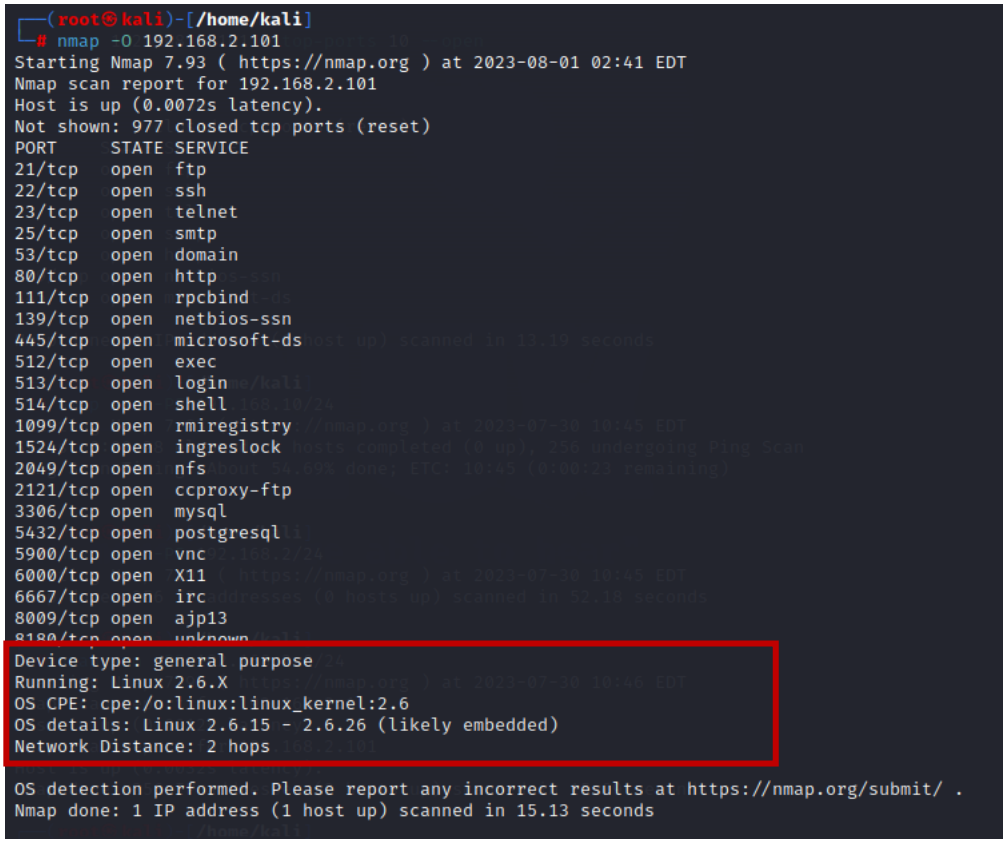
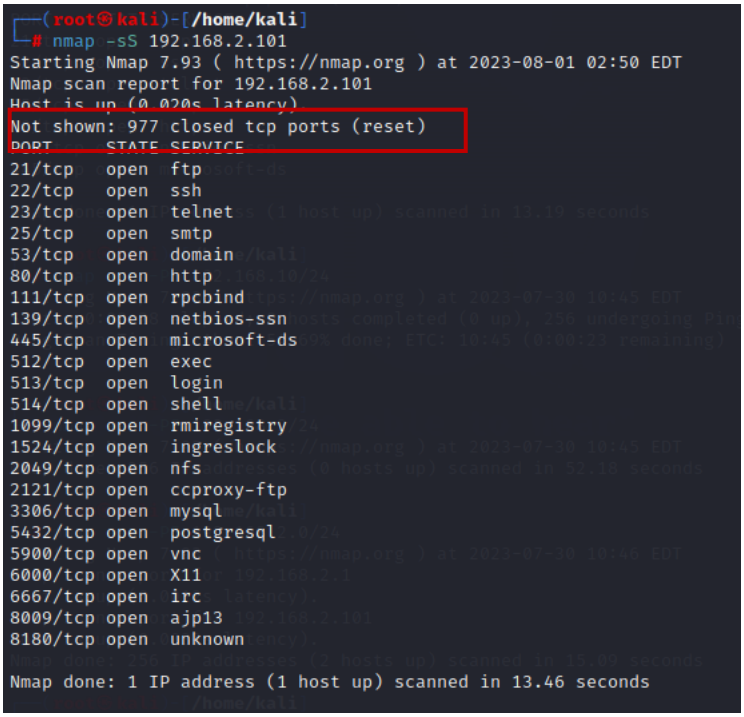
Eseguiamo le scansioni richieste sulla macchina metasploitable IP 192.168.2.101

OS fingerprint tramite comando **nmap -O <ip_target>** che ci permette di stimare il tipo di SO che ci risponde.

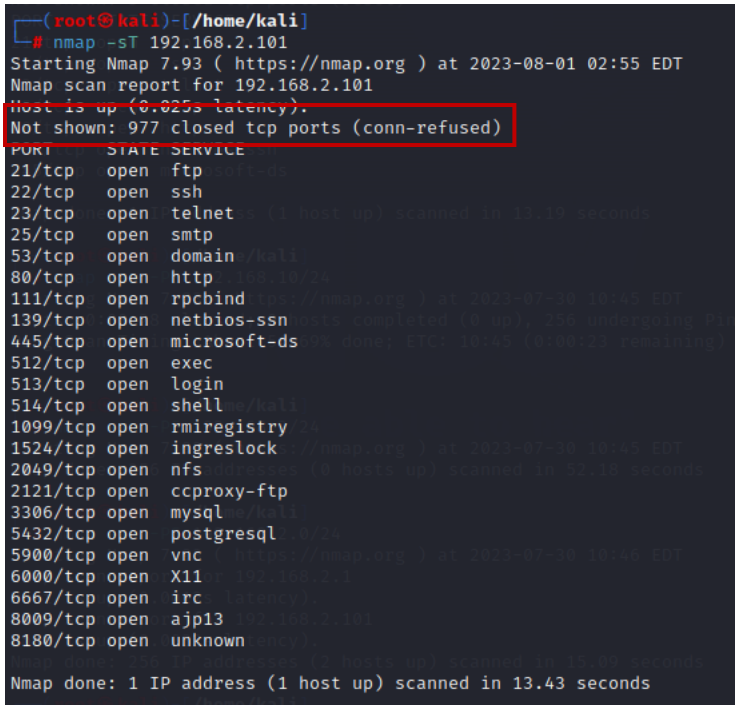


Poi eseguiamo una SYN scan tramite comando **nmap -sS <ip_target>** che invece ci fornisce informazioni su quali porte sono aperte, chiuse o filtrate da un firewall, inoltre questo tipo di scansione non porta a termine la connessione (three-way-handshake) rendendola così più difficile da rilevare.

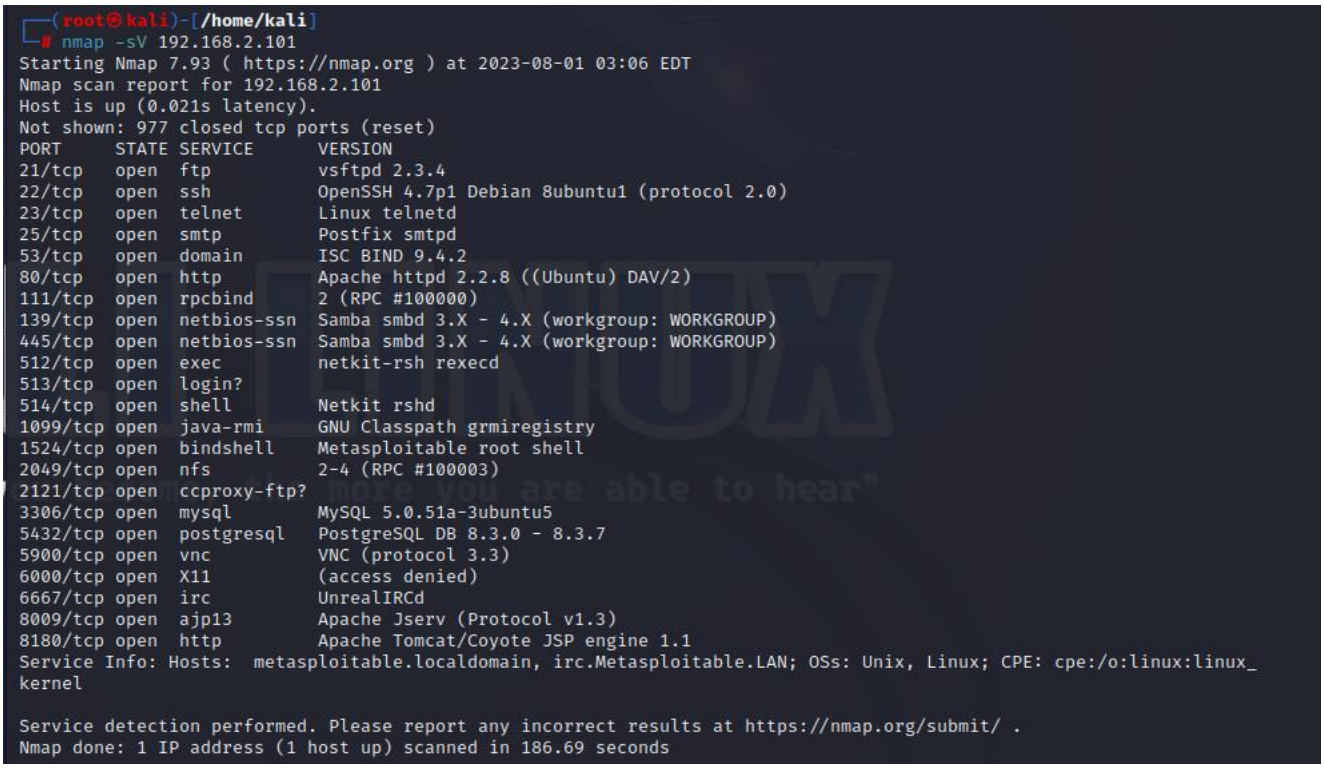


Eseguiamo poi una scansione TCP che invece porta a termine la connessione ciò richiede la completa apertura e chiusura della connessione. Infatti possiamo notare una differenza dalla connessione SYN ovvero che le porte chiuse vengono definite da connessione rifiutata invece nella scansione SYN non vendendo completata la connessione la

risposta delle porte avvine tramite protocollo RST che indica che la connessione non è stata accettata e quindi la porta non è in ascolto e non risponde con un pacchetto SYN-ACK quindi la differenza principale è che il pacchetto TCP RST è inviato in risposta a una connessione attiva, mentre il rifiuto di connessione è inviato in risposta a una richiesta di connessione che non è ancora stata stabilita.



Eseguiamo infine una scansione della versione dei servizi in ascolto tramite comando **nmap -sV <ip_target>**



Dopo aver impostato entrambi i target (metasploitable e kali) sulla stessa rete (1.0/24) eseguo una scansione della rete per identificare gli hosts attivi sulla stessa e conoscere il loro IP.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 04:20 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
MAC Address: 08:00:27:F3:4E:2E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.103
Host is up (0.00084s latency).
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.95 seconds
```

Vedo così che ci sono 3 host attivi di cui 2 macchine (virtual box) ed eseguo una scansione degli IP per capire di quali macchine si tratta(sistema operativo), quali sono le porte attive e la versione dei servizi.

Inizio dall'IP .1.101 dove vedo che tutte le porte sono chiuse non ci sono servizi in ascolto (causa firewall), inoltre nmap non mi identifica il SO, quindi riesco solo a capire che la macchina è attiva.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 04:14 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Eseguendo poi una scansione del secondo IP .1.103 ottengo invece più informazioni, vediamo che tipo di sistema operativo è la macchina scansionata: metaspoitable, Unix, Linux; poi abbiamo informazioni riguardo le porte aperte e la versione dei servizi attivi, come il servizio web HTTP (80) viene utilizzato per fornire pagine web che potrebbe contenere vulnerabilità o la porta 3306 mysql che è un sistema di gestione database e potrebbe anch'esso essere vulnerabile .

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 04:16 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.03 seconds
```