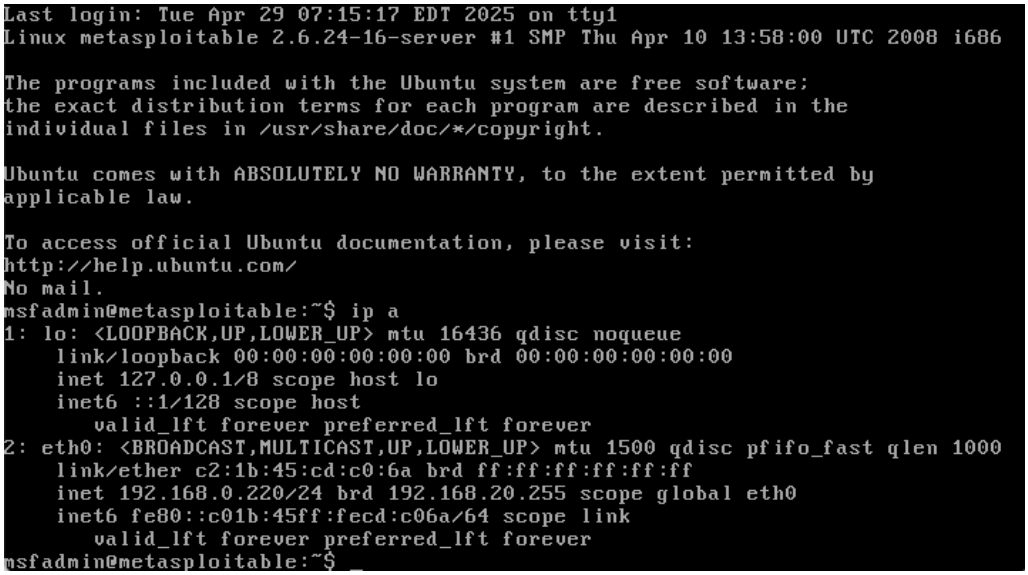
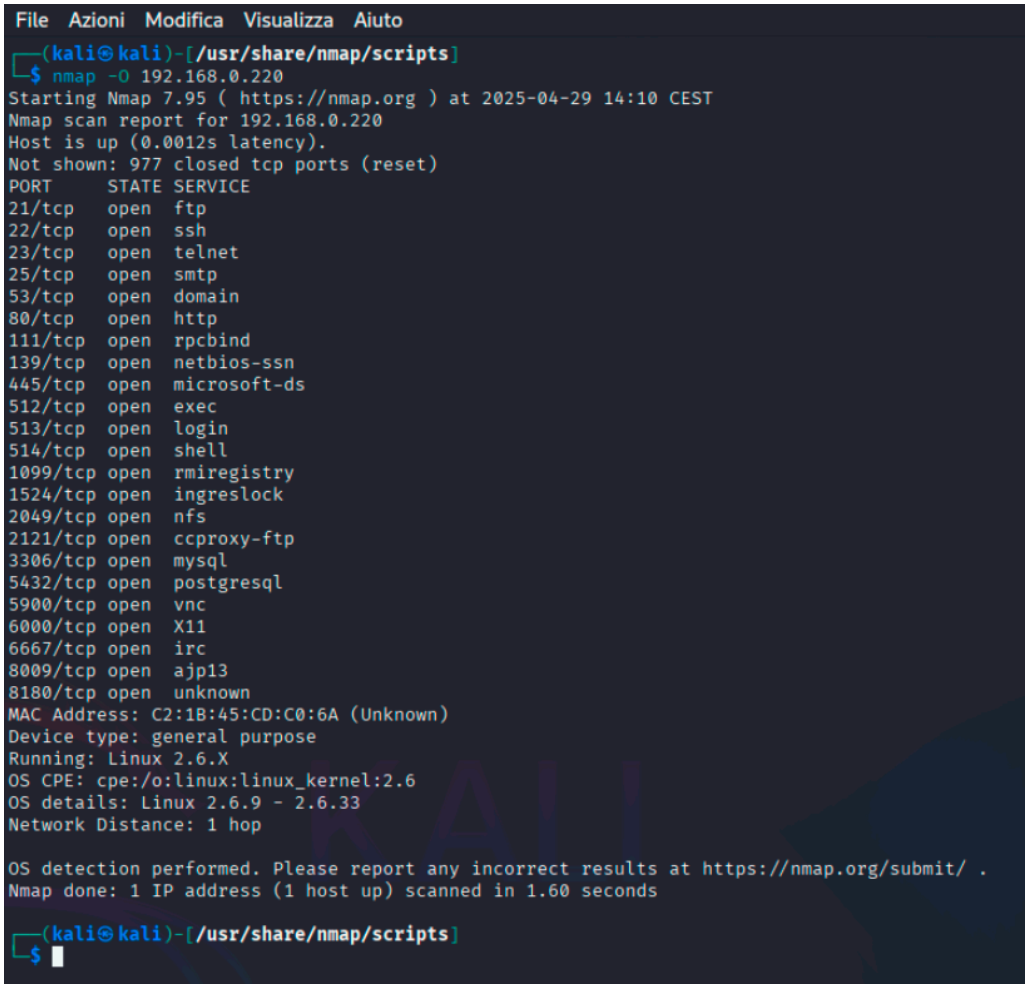
Reporto Esercitazione S5/L2

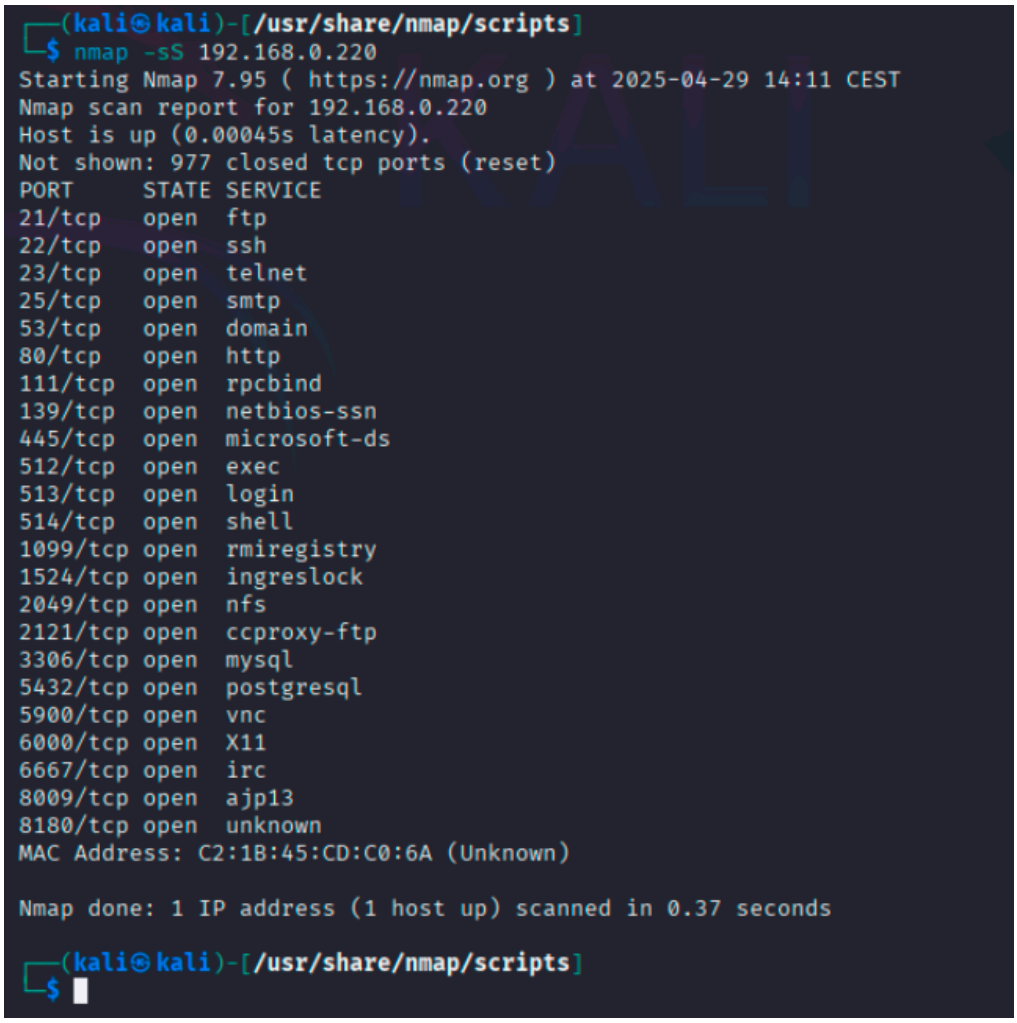
Metasploitable 192.168.0.220




Nmap -O 192.168.0.220 per fare check sulle porte e trovarmi l’os.



nmap -sS 192.168.0.220 per fare un check sulle porte.



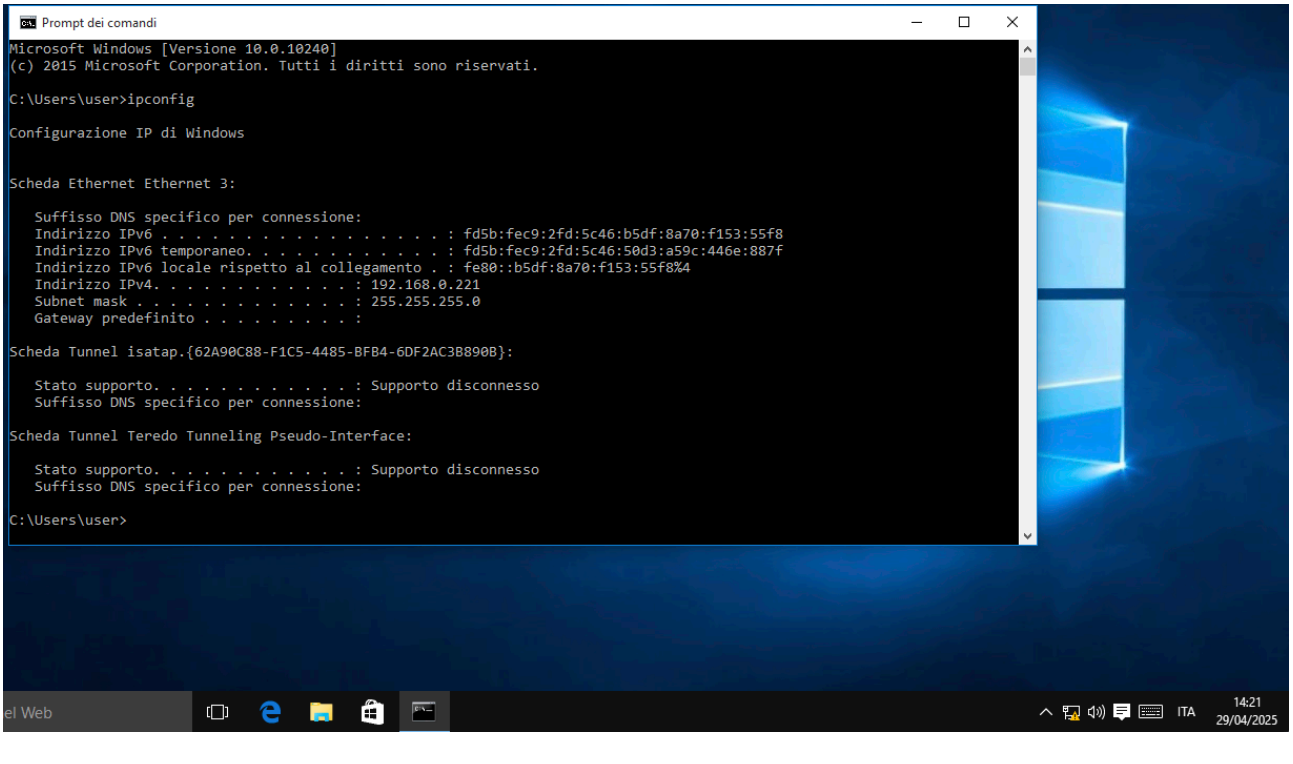

Tra Tcp e Syn non ci sono differenze sostanziali. L’unica differenza è il comando che si utilizza.

Nmap -sV 192.168.0.220 per trovarmi le versioni dei servizi attivi sull’ ip target.

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap -sV 192.168.0.220
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:15 CEST
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 14:16 (0:00:04 remaining)
Nmap scan report for 192.168.0.220
Host is up (0.00036s 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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: C2:1B:45:CD:C0:6A (Unknown)
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 131.36 seconds
```

Configurazione scheda di rete pc Windows
Indirizzo ip : 192.168.0.221



Nmap -O 192.168.0.221 riesco a vedere i servizi con porte aperte e l'OS details.