

Reporto Esercitazione S5/L2

Metasploitable 192.168.0.220

```
Last login: Tue Apr 29 07:15:17 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether c2:1b:45:cd:c0:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.220/24 brd 192.168.20.255 scope global eth0
    inet6 fe80::c01b:45ff:fece:c06a/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

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

```
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[/usr/share/nmap/scripts]
$ nmap -O 192.168.0.220
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:10 CEST
Nmap scan report for 192.168.0.220
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: C2:1B:45:CD:C0:6A (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds

(kali@kali)-[/usr/share/nmap/scripts]
$
```

nmap -sS 192.168.0.220 per fare un check sulle porte.

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ nmap -sS 192.168.0.220
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:11 CEST
Nmap scan report for 192.168.0.220
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: C2:1B:45:CD:C0:6A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

(kali㉿kali)-[/usr/share/nmap/scripts]
$
```

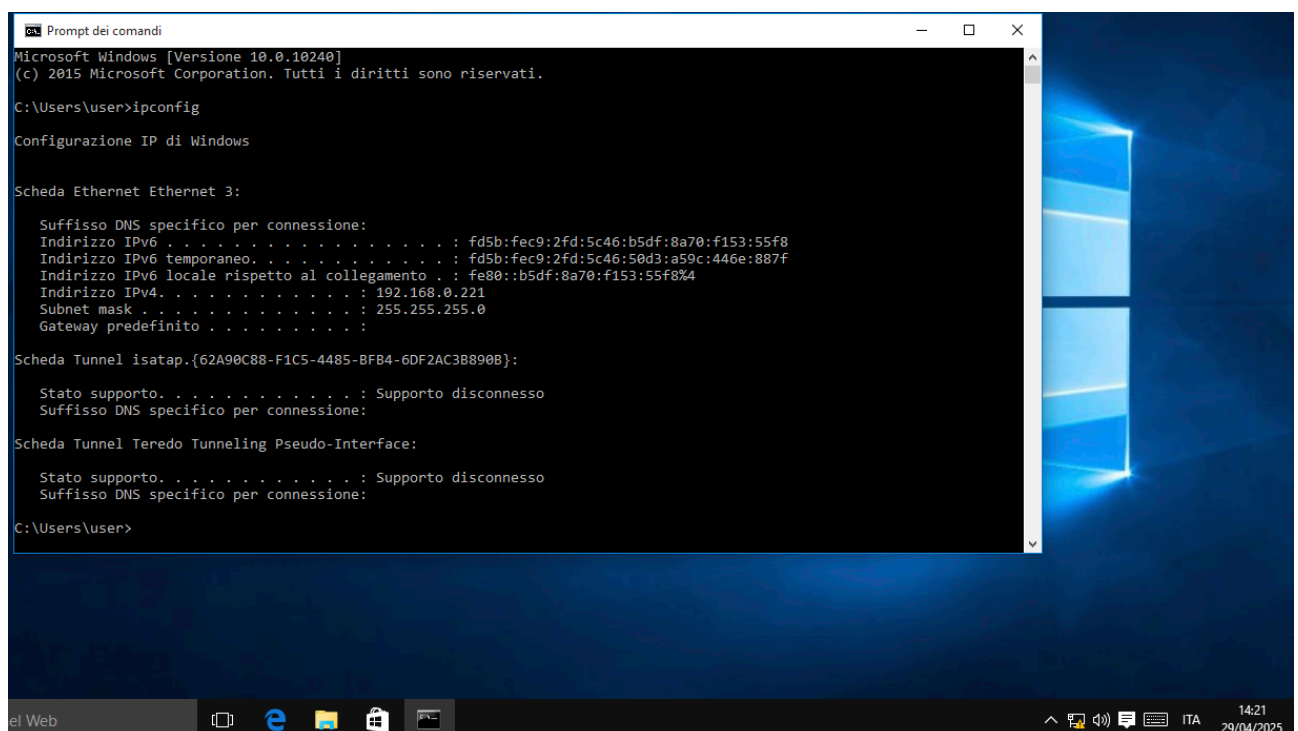
Tra Tcp e Syn non ci sono differenze sostanziali. L'unica differenza è il comando che si utilizza.

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.

```
(kali㉿kali)-[~]  
$ nmap -O 192.168.0.221  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:26 CEST  
Nmap scan report for 192.168.0.221  
Host is up (0.0011s latency).  
Not shown: 981 closed tcp ports (reset)  
PORT      STATE SERVICE  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1801/tcp  open  msmq  
2103/tcp  open  zephyr-clt  
2105/tcp  open  eklogin  
2107/tcp  open  msmq-mgmt  
3389/tcp  open  ms-wbt-server  
5357/tcp  open  wsdapi  
5432/tcp  open  postgresql  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
8443/tcp  open  https-alt  
MAC Address: 76:81:41:C0:F0:5F (Unknown)  
Device type: general purpose  
Running: Microsoft Windows 10  
OS CPE: cpe:/o:microsoft:windows_10  
OS details: Microsoft Windows 10 1507 - 1607  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```