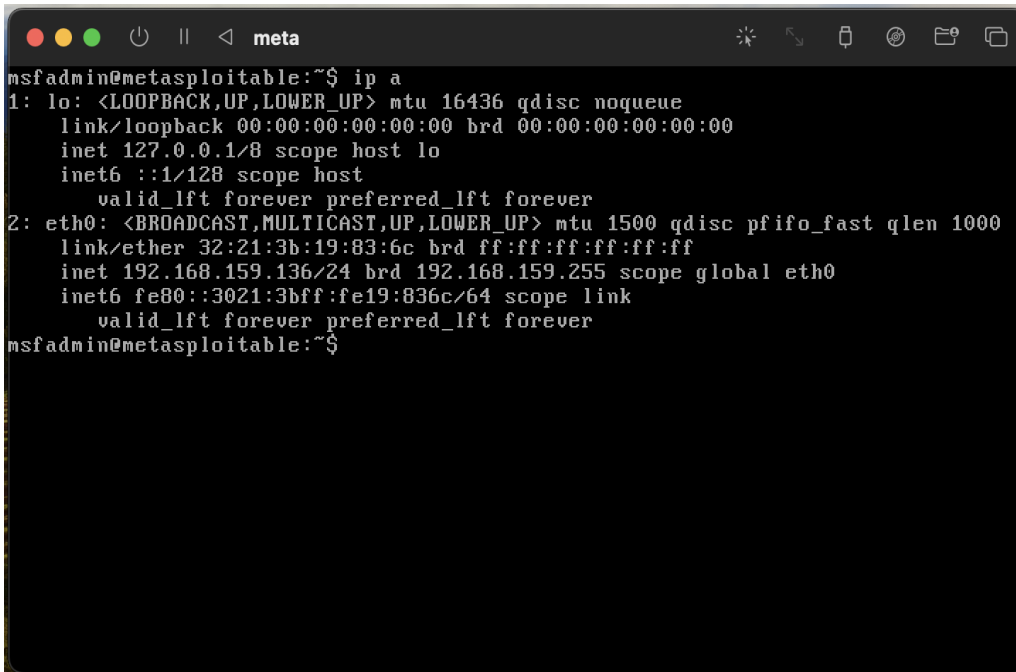
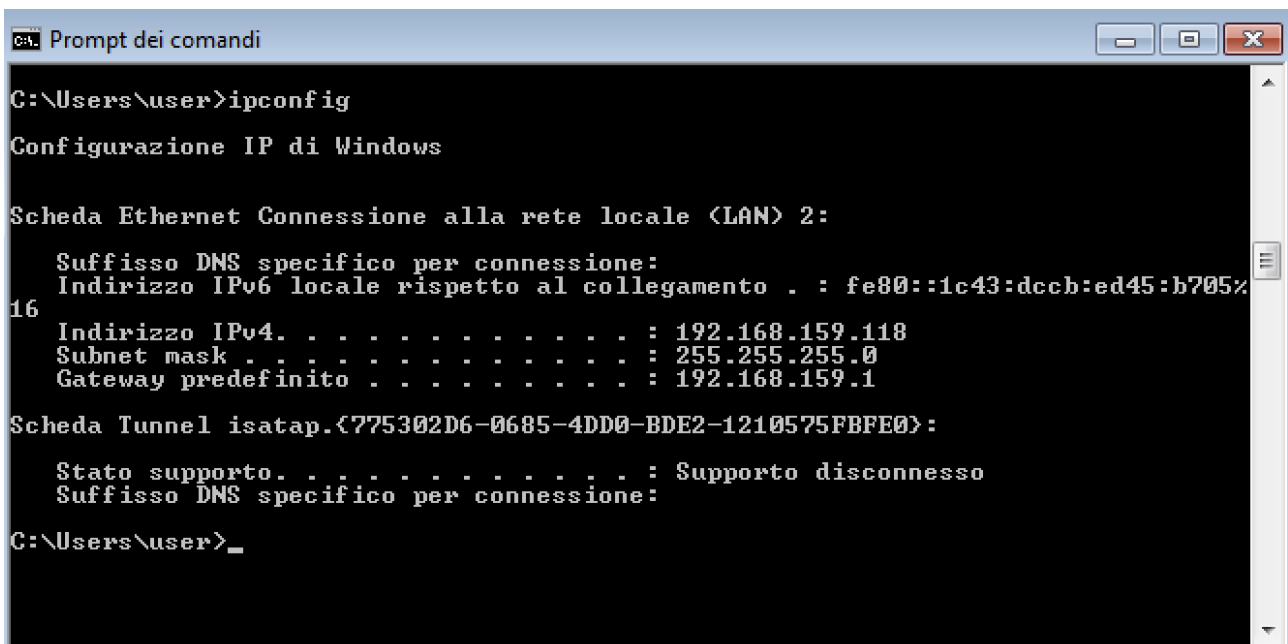


## Report Scansioni NMAP



```
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 32:21:3b:19:83:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.159.136/24 brd 192.168.159.255 scope global eth0
    inet6 fe80::3021:3bff:fe19:836c/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Con questo Screenshot si mostra l'indirizzo IP (192.168.159.136) della macchina **Metasploitable**.



```
C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN) 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::1c43:dcdb:ed45:b705%16
    Indirizzo IPv4. . . . . : 192.168.159.118
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.159.1

Scheda Tunnel isatap.{775302D6-0685-4DD0-BDE2-1210575FBFE0}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\user>
```

In questo caso si mostra l'indirizzo IP (192.168.159.118) della macchina **Windows 7**.

## OS Fingerprinting Metasploitable

```
kali@kali2023: ~  
File Actions Edit View Help  
(kali@kali2023)-[~]  
$ sudo nmap -O 192.168.159.136  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:47 CET  
Nmap scan report for 192.168.159.136  
Host is up (0.0016s latency).  
Not shown: 978 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
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: 32:21:3B:19:83:6C (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 1.53 seconds
```

Qui si è eseguito l'OS Fingerprinting su IP di Metasploitable.  
Possiamo notare quali porte risultano aperte, tra le quali:  
23(telnet);80(http) che possono risultare vulnerabili.  
Questa scan ci mostra anche i dettagli del Sistema Operativo di  
Metasploitable: Linux.

## SYN scan Metasploitable

```
kali@kali2023: ~  
File Actions Edit View Help  
  
(kali@kali2023)-[~]  
$ sudo nmap -sS 192.168.159.136  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:48 CET  
Nmap scan report for 192.168.159.136  
Host is up (0.00071s latency).  
Not shown: 978 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
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: 32:21:3B:19:83:6C (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds  
  
(kali@kali2023)-[~]  
$
```

Questa è la scan SYN che mostra, come la precedente scan, le porte aperte che si confermano le stesse.

## Scansione '-sT' Metasploitable

```
kali@kali2023: ~  
File Actions Edit View Help  
  
(kali@kali2023)-[~]  
$ sudo nmap -sT 192.168.159.136  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:48 CET  
Nmap scan report for 192.168.159.136  
Host is up (0.0012s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
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: 32:21:3B:19:83:6C (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds  
  
(kali@kali2023)-[~]  
$
```

Questa scan eseguita con -sT è in genere più invasiva rispetto alla precedente ma conferma comunque le stesse porte aperte.

## Version detection Metasploitable

```
kali@kali2023: ~  
File Actions Edit View Help  
  
(kali@kali2023)-[~]  
$ sudo nmap -sV 192.168.159.136  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:48 CET  
Nmap scan report for 192.168.159.136  
Host is up (0.00068s latency).  
Not shown: 978 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  
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        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
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: 32:21:3B:19:83:6C (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 12.31 seconds  
  
(kali@kali2023)-[~]  
$
```

La version detection di nmap ci fornisce i servizi e le versioni dei software in ascolto sulle porte che risultano aperte.

## OS Fingerprinting Windows

```
kali@kali2023: ~  
File Actions Edit View Help  
  
(kali@kali2023)-[~]  
$ sudo nmap -O 192.168.159.118  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 09:53 CET  
Nmap scan report for 192.168.159.118  
Host is up (0.0031s latency).  
Not shown: 993 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
554/tcp    open  rtsp  
2869/tcp   open  iclslap  
5357/tcp   open  wsddapi  
10243/tcp  open  unknown  
MAC Address: 3A:7D:20:A9:FC:DB (Unknown)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: specialized|phone  
Running: Microsoft Windows 7|Phone  
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows  
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0  
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 6.66 seconds  
  
(kali@kali2023)-[~]  
$
```

Questa è la scan su OS Fingerprinting sulla macchina Windows 7.

Rispetto alla scansione effettuata su Metasploitable possiamo notare come le porte aperte siano di meno.

Questo fattore può essere dovuto dal fatto che sul sistema windows siano presenti Firewall che bloccano le porte e non permette di vederle una volta effettuata la scansione.