

# -EJERCICIOS ESCANER NMAP-

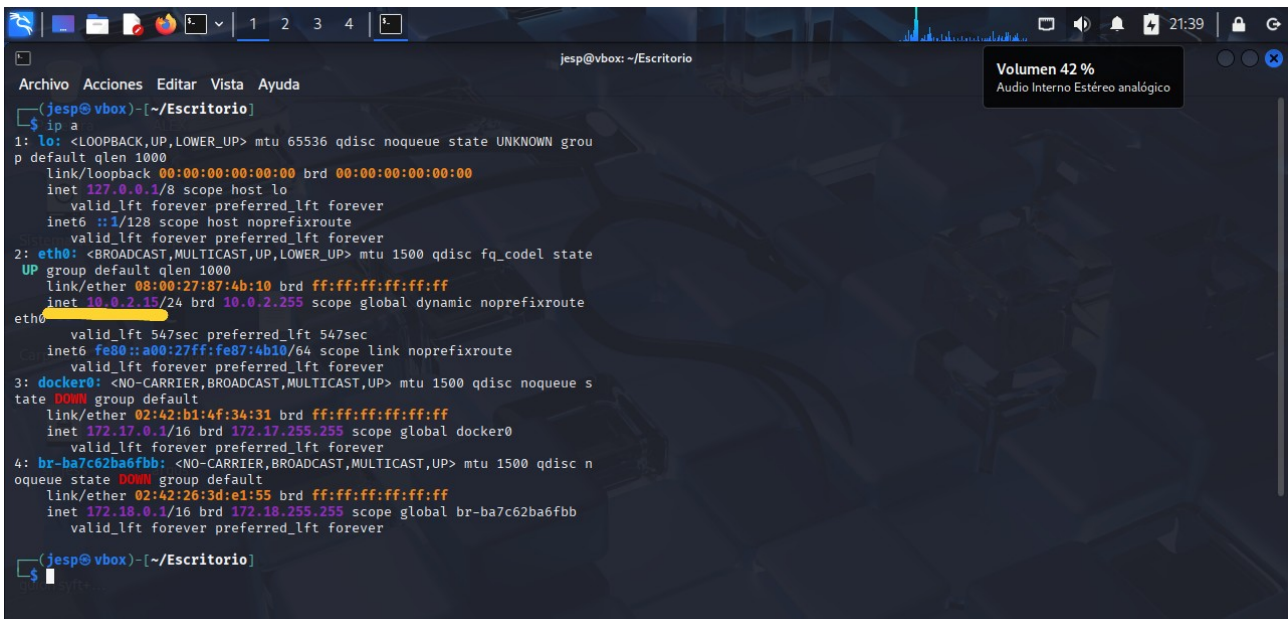
## • PRERREQUISITOS Y CONFIGURACIÓN

### Requisitos:

- **Kali Linux y Metasploitable2** funcionando como máquinas virtuales en VirtualBox.
- Ambas configuradas con:  
Red > Adaptador 1 > Red NAT > NatNetwork.

### Verifica IPs y conectividad:

# En Kali  
*ip a*



```
(jesp@vbox)~[/Escritorio]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:87:4b:10 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
        valid_lft 547sec preferred_lft 547sec
    inet6 fe80::a00:27ff:fe87:4b10/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b1:4f:34:31 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
4: br-ba7c62ba6fbb: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:26:3d:e1:55 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-ba7c62ba6fbb
        valid_lft forever preferred_lft forever
(jesp@vbox)~[/Escritorio]
$
```

# En Metasploitable2  
*ifconfig*

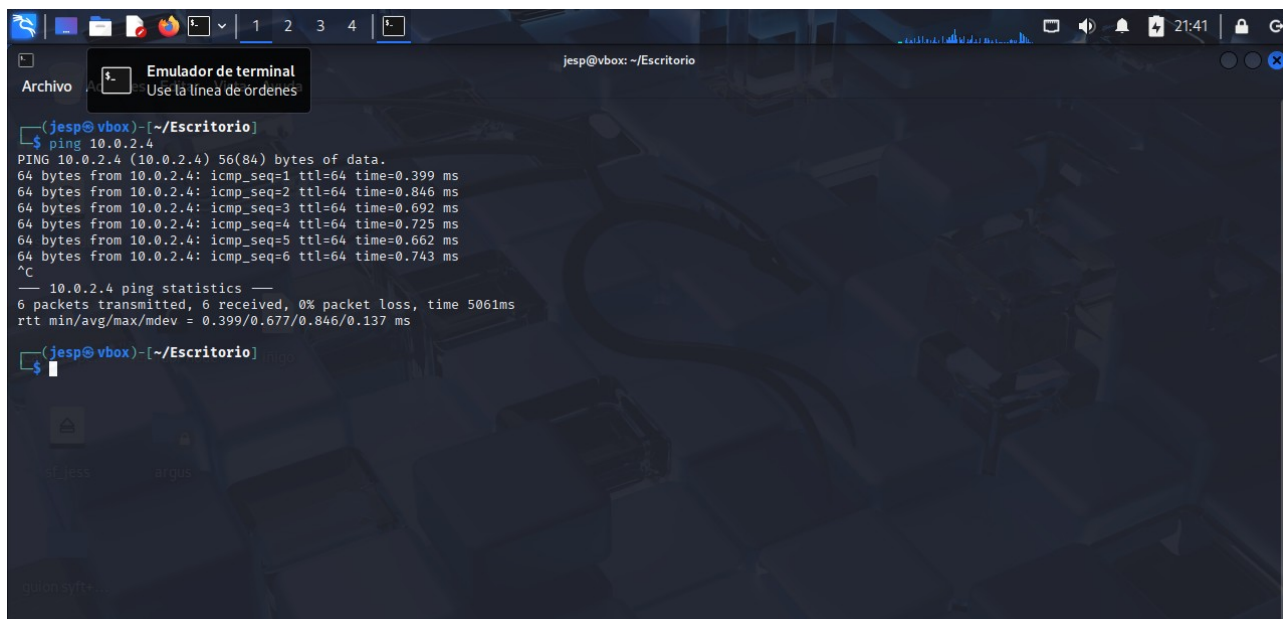
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:6f:e0
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe23:6fe0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4730 (4.6 KB)  TX bytes:7170 (7.0 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$ _
```

# Comprobar conectividad  
*ping <IP\_Metasploitable2>*

*ping 10.0.2.4*



The screenshot shows a terminal window titled "Emulador de terminal" with the prompt "jesp@vbox: ~/Escritorio". The user has entered the command "ping 10.0.2.4". The output shows six successful ping requests, each receiving 64 bytes of data from 10.0.2.4 with varying times. The statistics at the bottom indicate 6 packets transmitted, 6 received, 0% packet loss, and a total time of 5061ms.

```
(jesp@vbox)~[/Escritorio]
$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.399 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.846 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.692 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.725 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.662 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.743 ms
^C
--- 10.0.2.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5061ms
rtt min/avg/max/mdev = 0.399/0.677/0.846/0.137 ms
(jesp@vbox)~[/Escritorio]
```

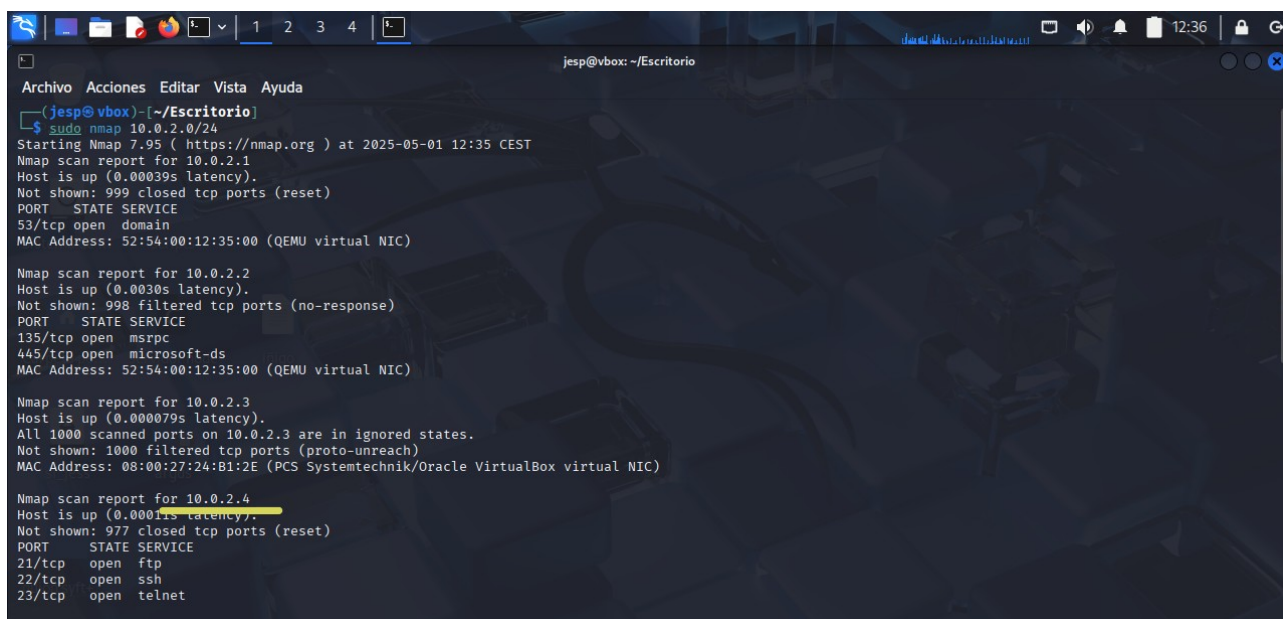
## EJERCICIO 1 - Descubrir equipos en la red NAT

Comandos:

a) *sudo nmap 10.0.2.0/24*

b) *sudo nmap 10.0.2.0-255*

c) *sudo nmap -sn 10.0.2.4*



The screenshot shows a terminal window titled "Emulador de terminal" with the prompt "jesp@vbox: ~/Escritorio". The user has entered the command "sudo nmap 10.0.2.0/24". The output shows the Nmap scan report for 10.0.2.1, 10.0.2.2, 10.0.2.3, and 10.0.2.4. The scan for 10.0.2.1 shows 53/tcp open domain. The scan for 10.0.2.2 shows 135/tcp open msrpc and 445/tcp open microsoft-ds. The scan for 10.0.2.3 shows all 1000 scanned ports in ignored states. The scan for 10.0.2.4 shows 21/tcp open ftp, 22/tcp open ssh, and 23/tcp open telnet.

```
(jesp@vbox)~[/Escritorio]
$ sudo nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 12:35 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.000079s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:24:B1:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0001s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
```

```
jesp@vbox: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
(jesp@vbox)~[~/Escritorio]
$ sudo nmap 10.0.2.0-255
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 12:37 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00061s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsdaapi
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.000075s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:24:B1:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.00010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
```

```
jesp@vbox: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
(jesp@vbox)~[~/Escritorio]
$ sudo nmap -sn 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 12:51 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00024s latency).
MAC Address: 08:00:27:23:6F:E0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds

(jesp@vbox)~[~/Escritorio]
$
```

## Explicación:

- `-sn`: escaneo tipo "ping sweep", sin escanear puertos, solo detecta hosts vivos. Realiza un escaneo en blanco (no escanea puertos), ideal para descubrir hosts en una red sin necesidad de ping ICMP.
- Así verificas si Metasploitable2 aparece.

### Alternativas para redes NAT:

- `nmap -PR`:

Realiza un ping de ARP, que es una alternativa a los ping ICMP en redes NAT.

- `nmap -sN`:

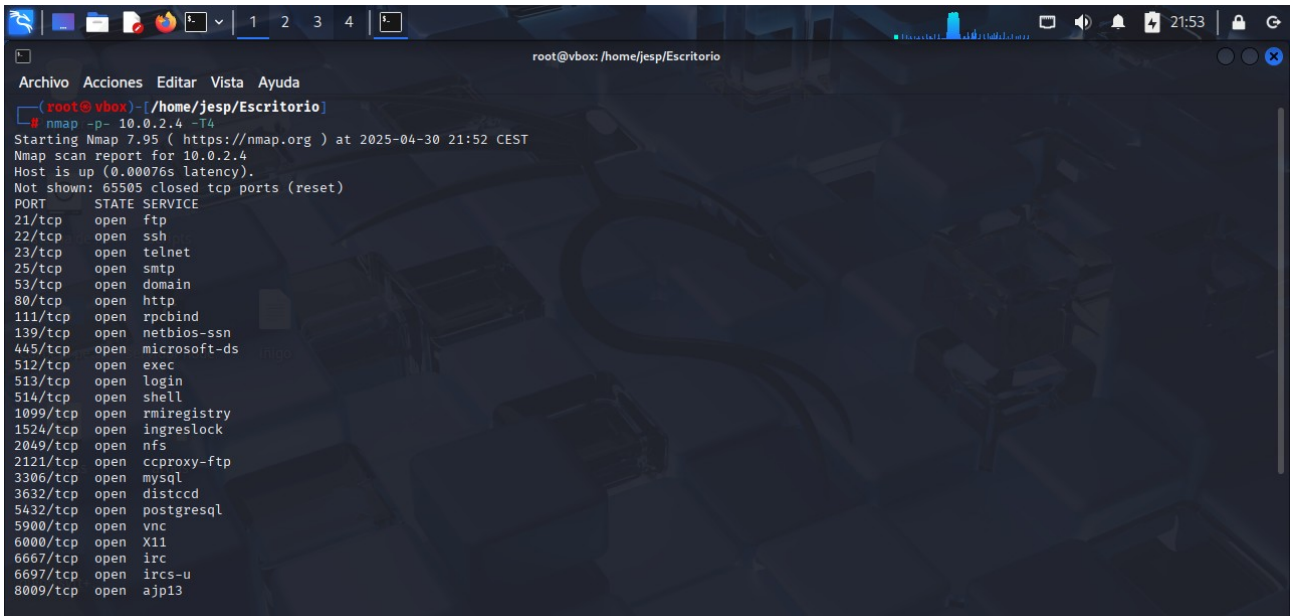
Realiza un escaneo TCP SYN (escaneo de detección de hosts), que también es efectivo en redes NAT.



## EJERCICIO 2 - Escaneo de puertos de Metasploitable2

Comando:

```
sudo nmap -p- 10.0.2.4 -T4
```



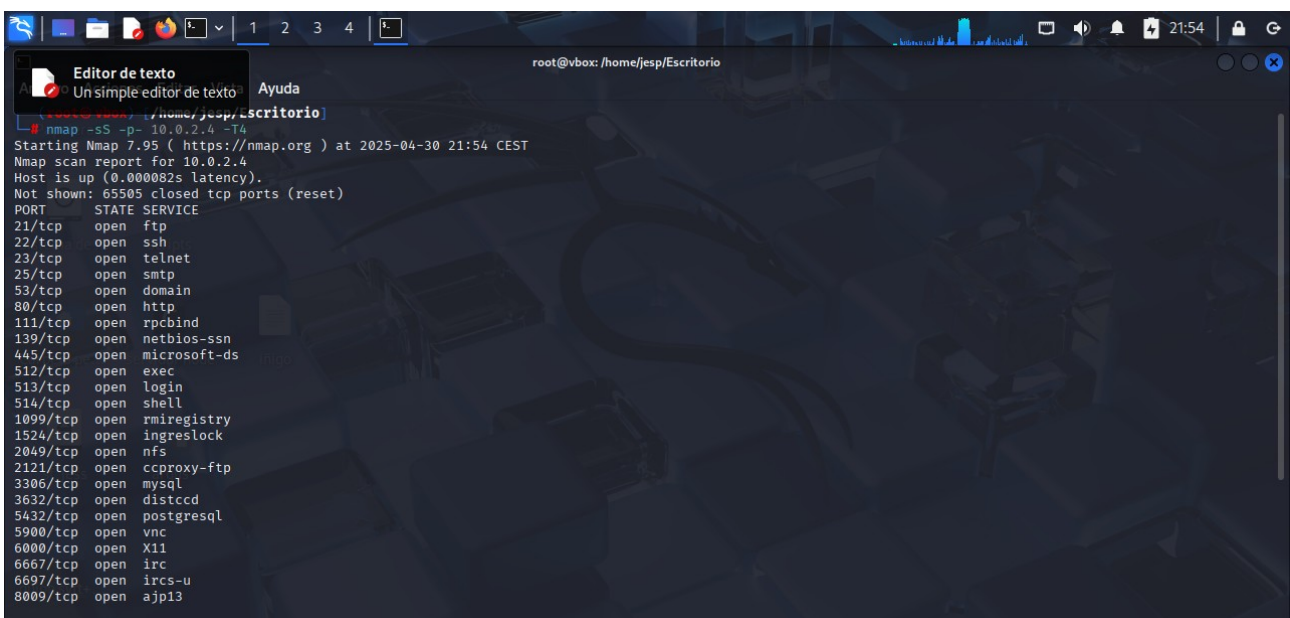
```
root@vbox: /home/jesp/Escritorio
Archivo Acciones Editar Vista Ayuda
root@vbox:~# sudo nmap -p- 10.0.2.4 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 21:52 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00076s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
```

Explicación:

- -p-: escanea todos los puertos (0–65535).
- -T4: aumenta la velocidad del escaneo (útil para redes locales).

Alternativamente:

```
sudo nmap -sS -p- 10.0.2.4
```



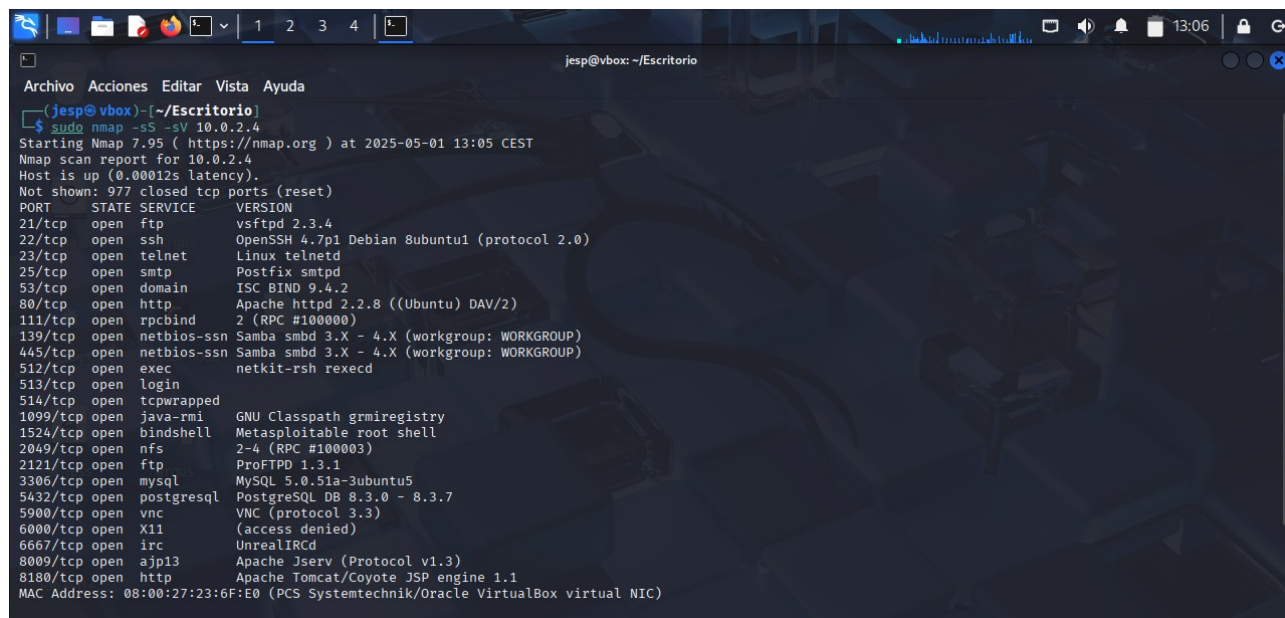
```
root@vbox: /home/jesp/Escritorio
Editor de texto
Un simple editor de texto
Ayuda
root@vbox:~# sudo nmap -sS -p- 10.0.2.4 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 21:54 CEST
Nmap scan report for 10.0.2.4
Host is up (0.000082s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
```

- -sS: escaneo TCP SYN (sigiloso y rápido).

## EJERCICIO 3 - Esquema de puertos, estado y servicios

Comando:

```
sudo nmap -sS -sV 10.0.2.4
```

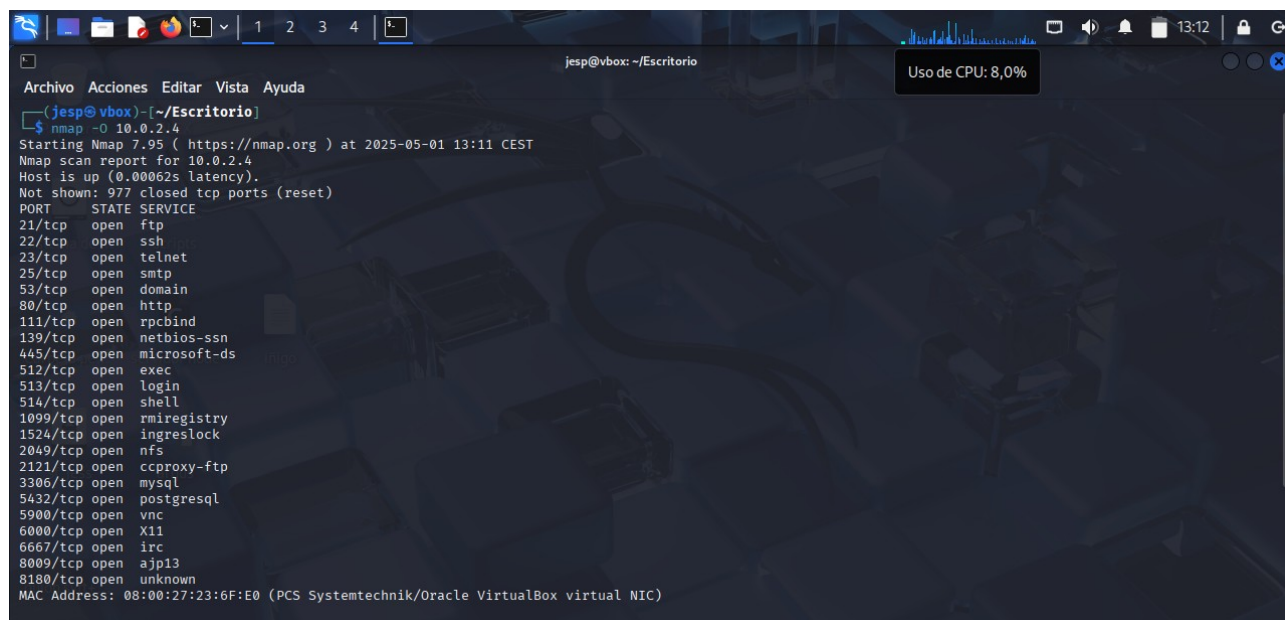


```
Archivo Acciones Editar Vista Ayuda
(jesp@ vbox) - [~/Escritorio]
$ sudo nmap -sS -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 13:05 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
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  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: 08:00:27:23:6F:E0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

## EJERCICIO 4 - Detección del sistema operativo

Comando:

```
nmap -O 10.0.2.4
```



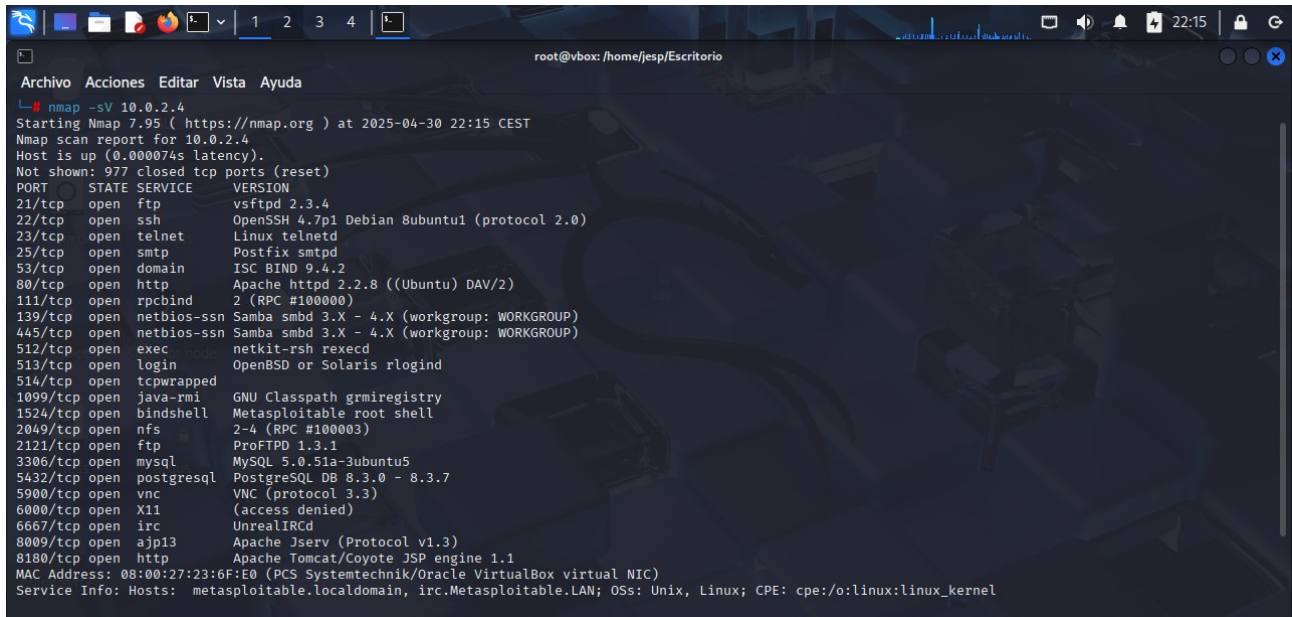
```
Archivo Acciones Editar Vista Ayuda
(jesp@ vbox) - [~/Escritorio]
$ nmap -O 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-01 13:11 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    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  microsoft-ds Microsoft Windows [v6.0.6002]
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp  ccproxy-ftp 1.1.1
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  unknown
MAC Address: 08:00:27:23:6F:E0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Explicación:

- -O: detección del sistema operativo usando fingerprinting de paquetes TCP/IP.

## EJERCICIO 5 - Añadir versión de servicios al esquema

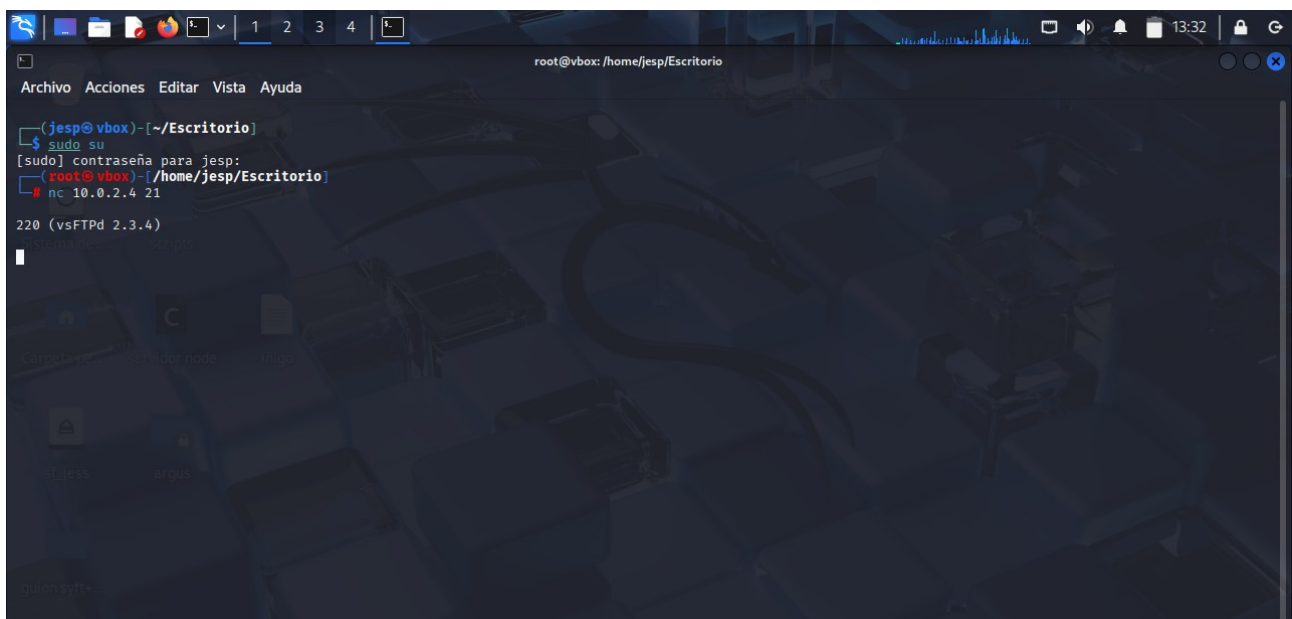
`sudo nmap -sV 10.0.2.4`



```
root@vbox: /home/jesp/Escritorio
Archivo Acciones Editar Vista Ayuda
└─$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 22:15 CEST
Nmap scan report for 10.0.2.4
Host is up (0.000074s 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        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: 08:00:27:23:6F:E0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

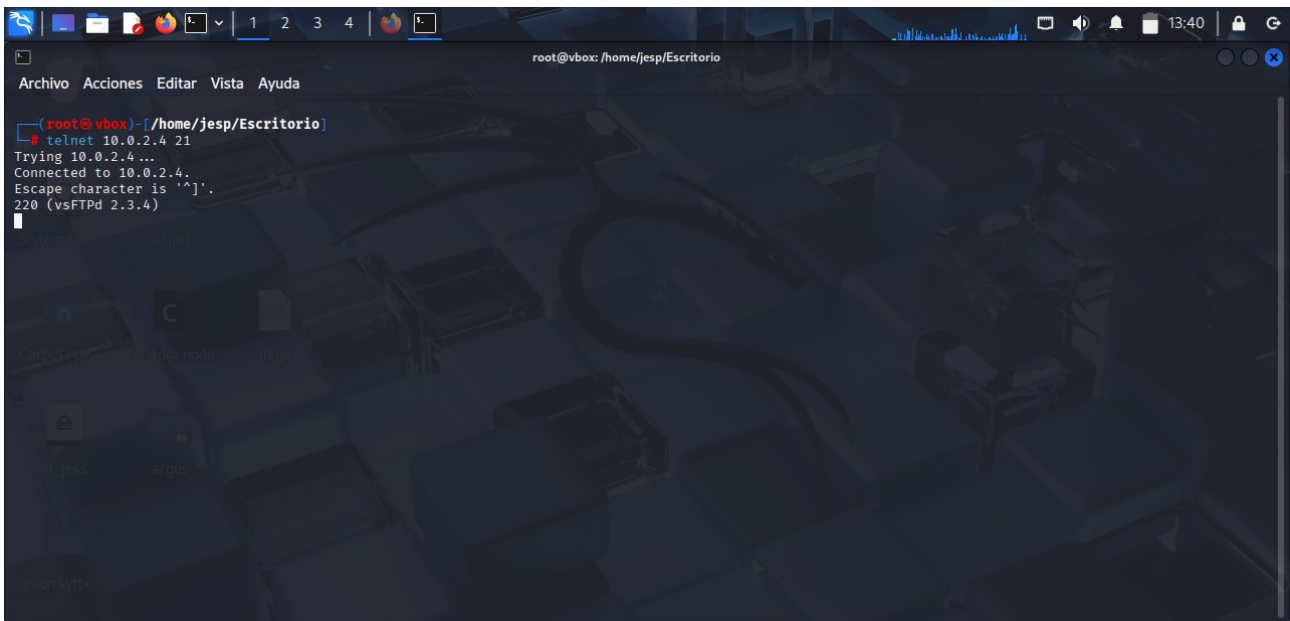
## EJERCICIO 6 - Verificar versión manualmente con nc, telnet y navegador

### 1. Ftp (21)



```
root@vbox: /home/jesp/Escritorio
Archivo Acciones Editar Vista Ayuda
└─$ sudo su
[sudo] contraseña para jesp:
root@vbox: /home/jesp/Escritorio
└─$ nc 10.0.2.4 21
220 (vsFTPd 2.3.4)
```

## 2. Telnet

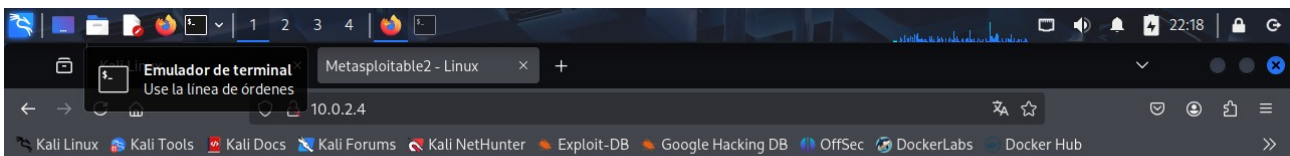


Resultado típico:

220 (vsFTPd 2.3.4)

## 3. Navegador

<http://10.0.2.4>



metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



## EJERCICIO 7 - Análisis de vulnerabilidades SSH con Nmap NSE

Instalamos scripts *vulscan* y/o *vulners*:

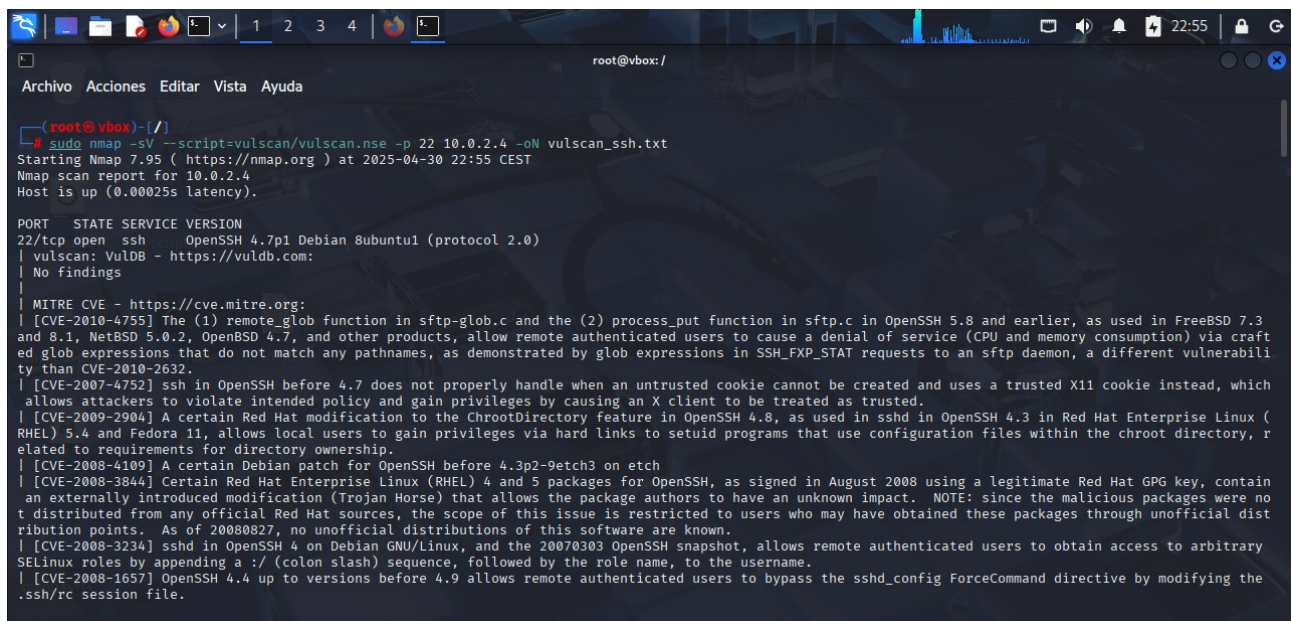
`cd /usr/share/nmap/scripts/`

- `sudo git clone https://github.com/scipag/vulscan`
- `sudo git clone https://github.com/vulnersCom/nmap-vulners.git`

Ambos resultados listan CVEs conocidos del servicio SSH.

### Comando 1: vulscan

`sudo nmap -sV --script=vulscan/vulscan.nse -p 22 10.0.2.4 -oN vulscan_ssh.txt`



```
root@vbox: /  
Archivo Acciones Editar Vista Ayuda  
root@vbox:~# sudo nmap -sV --script=vulscan/vulscan.nse -p 22 10.0.2.4 -oN vulscan_ssh.txt  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 22:55 CEST  
Nmap scan report for 10.0.2.4  
Host is up (0.00025s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| vulscan: VulDB - https://vuldb.com:  
| No findings  
|  
| MITRE CVE - https://cve.mitre.org:  
| [CVE-2010-4755] The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3  
| and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via craft  
| ed glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerabili  
| ty than CVE-2010-2632.  
| [CVE-2007-4752] ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which  
| allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.  
| [CVE-2009-2904] A certain Red Hat modification to the ChrootDirectory feature in OpenSSH 4.8, as used in sshd in OpenSSH 4.3 in Red Hat Enterprise Linux (R  
| HEL) 5.4 and Fedora 11, allows local users to gain privileges via hard links to setuid programs that use configuration files within the chroot directory, r  
| elated to requirements for directory ownership.  
| [CVE-2008-4109] A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch  
| [CVE-2008-3844] Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain  
| an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were no  
| t distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial dist  
| ribution points. As of 20080827, no unofficial distributions of this software are known.  
| [CVE-2008-3234] sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary  
| SELinux roles by appending a :/ (colon slash) sequence, followed by the role name, to the username.  
| [CVE-2008-1657] OpenSSH 4.4 up to versions before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the  
| .ssh/rc session file.
```

### Comando 2: vulners

`sudo nmap -sV --script=vulners -p 22 10.0.2.4 -oN vulners_ssh.txt`



```
Archivo Acciones Editar Vista Ayuda
(root@vbox)-[/]
# sudo nmap -sV --script=vulners -p 22 10.0.2.4 -oN vulners_ssh.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 22:56 CEST
Nmap scan report for 10.0.2.4
Host is up (0.00022s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
vulners:
cpe:/a:openbsd:openssh:4.7p1:
2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8 https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 *EXPLOIT*
0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
PACKETSTORM:94556 7.8 https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 7.8 https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 *EXPLOIT*
EXPLOITPACK:67F6569F63A082199721C069C8528BD7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C8528BD7 *EXPLOIT*
EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
EDB-ID:24450 7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
EDB-ID:15215 7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
```

- Explicación:
- -sV: obtiene versiones de servicios.
  - --script=vulners: consulta la base de datos de vulnerabilidades.
  - -oN archivo.txt: guarda salida en archivo.
-