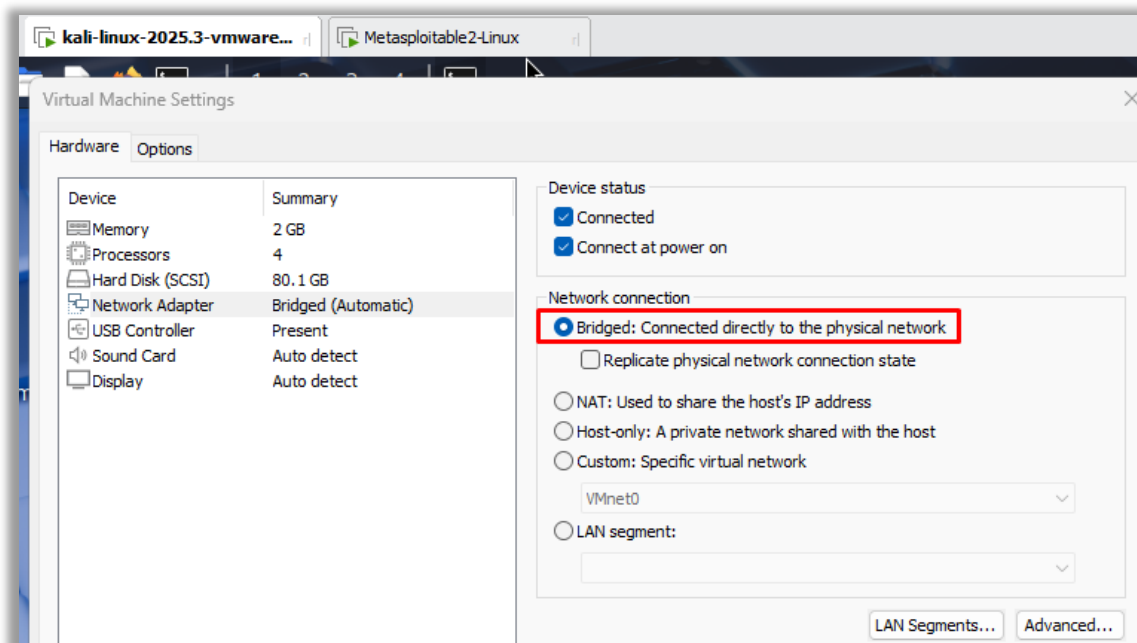


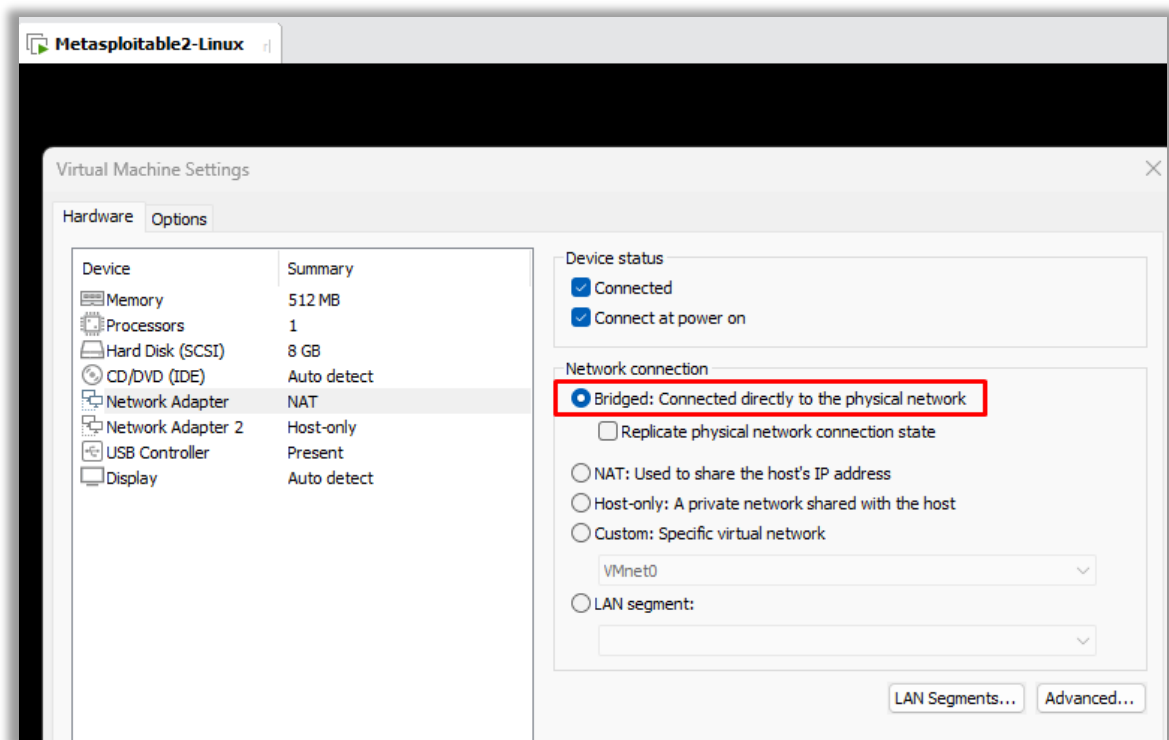
# Práctica: Escaneo y Mitigación de Vulnerabilidades en Metasploitable 2

## Parte 1: Configuración del Entorno

### 1.1 Instalación de Metasploitable 2

1. Descarga la imagen de Metasploitable 2 desde el sitio oficial de Rapid7.
2. Importa la imagen en VMware y configura la red en modo Puente o Bridge, para que pertenezcan a la misma red.





3. Inicia la máquina virtual y asegúrate de que tienes conectividad con tu máquina anfitriona, Kali y Metasploitable
4. Obten la IP de Metasploitable 2 con: ifconfig

```
kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.146 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::18b:f9cd:6745:9491 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:d0:35:37 txqueuelen 1000 (Ethernet)
    RX packets 449 bytes 35157 (34.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 326 bytes 33373 (32.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 40 bytes 3072 (3.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 3072 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:3e:6d:bb
          inet addr:192.168.1.147  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3e:6dbb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 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:4370 (4.2 KB)  TX bytes:7242 (7.0 KB)
          Interrupt:17 Base address:0x2000

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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _

```

Confirmación de Alcance de la Red con ping:

```

(kali㉿kali)-[~]
$ ping 192.168.1.147
PING 192.168.1.147 (192.168.1.147) 56(84) bytes of data:
64 bytes from 192.168.1.147: icmp_seq=1 ttl=64 time=0.773 ms
64 bytes from 192.168.1.147: icmp_seq=2 ttl=64 time=0.436 ms
64 bytes from 192.168.1.147: icmp_seq=3 ttl=64 time=0.488 ms
64 bytes from 192.168.1.147: icmp_seq=4 ttl=64 time=0.540 ms
64 bytes from 192.168.1.147: icmp_seq=5 ttl=64 time=0.442 ms
64 bytes from 192.168.1.147: icmp_seq=6 ttl=64 time=0.526 ms
^C
— 192.168.1.147 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5108ms
rtt min/avg/max/mdev = 0.436/0.534/0.773/0.113 ms

(kali㉿kali)-[~]
$ 

```

```

msfadmin@metasploitable:~$ ping 192.168.1.146
PING 192.168.1.146 (192.168.1.146) 56(84) bytes of data:
64 bytes from 192.168.1.146: icmp_seq=1 ttl=64 time=0.401 ms
64 bytes from 192.168.1.146: icmp_seq=2 ttl=64 time=0.683 ms
64 bytes from 192.168.1.146: icmp_seq=3 ttl=64 time=0.317 ms
64 bytes from 192.168.1.146: icmp_seq=4 ttl=64 time=0.555 ms
64 bytes from 192.168.1.146: icmp_seq=5 ttl=64 time=0.316 ms
64 bytes from 192.168.1.146: icmp_seq=6 ttl=64 time=0.477 ms
64 bytes from 192.168.1.146: icmp_seq=7 ttl=64 time=0.487 ms

--- 192.168.1.146 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5994ms
rtt min/avg/max/mdev = 0.316/0.462/0.683/0.123 ms
msfadmin@metasploitable:~$

```

## 1.2 Configuración de Herramientas de Escaneo

1. Verifica que **Nmap** y **Wireshark** estén correctamente instalados en el sistema anfitrión.

- En Linux, usa:

```

(kali@kali)-[~]
$ sudo apt update && sudo apt install nmap wireshark -y
[sudo] password for kali:
Get:1 http://archive-4.kali.org/kali kali-rolling InRelease [34.0 kB]
Get:2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://archive-4.kali.org/kali kali-rolling/main amd64 Contents (deb) [52.3 MB]
Fetched 73.3 MB in 8s (9,649 kB/s)
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
wireshark is already the newest version (4.4.9-1).
wireshark set to manually installed.
The following packages were automatically installed and are no longer required:
amass-common          libportmidi0         python3-bluepy        python3-protobuf
libbluray2            librav1e0.7          python3-click-plugins python3-zombie-imp
libbson-1.0-0t64      libtheoradec1        python3-gpg            samba-ad-dc
libjs-jquery-ui       libtheoraenc1        python3-kismetcapturebtgeiger  samba-ad-provision
libjs-underscore     libudfread0          python3-kismetcapturefreaklabszigbee  samba-dsdb-modules
libmongoc-1.0-0t64   libx264-164          python3-kismetcapturertl433
libmongocrypt0       libxml2              python3-kismetcaptureertladsb
libplacebo349         libyelp0             python3-kismetcaptureertlamr
Use 'sudo apt autoremove' to remove them.

```

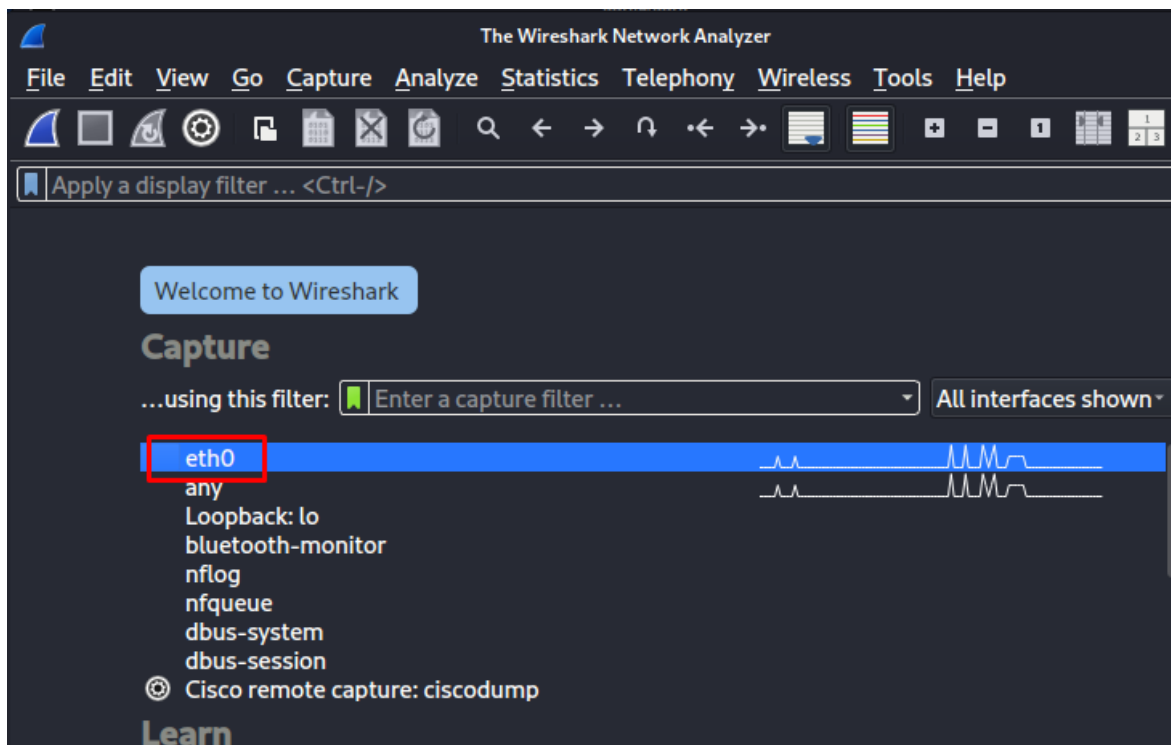
```

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 3

```

2. Asegúrate de que **Wireshark** esté configurado para capturar tráfico en la interfaz de red adecuada.

3. Asegúrate de tener configurado y listo **Git y GitHub** para gestionar la documentación



## Parte 2: Escaneo de Puertos y Servicios con Nmap

### 2.1 Escaneo de Puertos Básico (Identificación de Puertos Abiertos)

1. En la máquina anfitriona, abre una terminal y realiza un escaneo de todos los puertos de Metasploitable 2:

Utilizaremos el escaneo SYN (-sS), que es rápido y "sigiloso" (menos invasivo), para escanear todos los 65535 puertos (-p-).

```
(kali@kali)-[~]
$ nmap -sS -p- 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 15:54 EDT
Nmap scan report for 192.168.1.147
Host is up (0.0017s 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
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38109/tcp open  unknown
42123/tcp open  unknown
46354/tcp open  unknown
54997/tcp open  unknown
MAC Address: 00:0C:29:3E:6D:BB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
(kali@kali)-[~]
$
```

2. **Análisis de Resultados:** Examina los puertos abiertos e identifica los servicios principales, que incluirán:

**FTP (21), SSH (22), Telnet (23), HTTP (80), MySQL (3306).**

#### **Puertos Abiertos Identificados:**

- **21/tcp** (Servicio ftp)
- **22/tcp** (Servicio ssh)
- **23/tcp** (Servicio telnet)
- **80/tcp** (Servicio http)
- **3306/tcp** (Servicio mysql)

- Además, se encontraron otros servicios, como SMTP (25), DNS/Domain (53), y PostgreSQL (5432).

3. Tarea: Documenta los riesgos asociados a cada puerto abierto y servicio encontrado.

Puerto	Servicio	Riesgos Asociados
21/tcp	FTP	<b>Riesgo Crítico.</b> Se espera que sea la versión <b>vsftpd 2.3.4</b> , que contiene una <b>puerta trasera (backdoor)</b> que permite la ejecución de comandos remotos sin autenticación.
22/tcp	SSH	<b>Riesgo Alto.</b> Suele estar configurado para permitir el <i>login</i> como <i>root</i> con credenciales débiles o por defecto (msfadmin/msfadmin).
23/tcp	Telnet	<b>Riesgo Alto.</b> Telnet transmite toda la sesión, incluyendo credenciales (usuario y contraseña), <b>en texto plano (sin cifrar)</b> . Esto permite a un atacante en la misma red capturar fácilmente las credenciales con una herramienta como Wireshark.
80/tcp	HTTP	<b>Riesgo Alto.</b> Aloja aplicaciones web conocidas por ser vulnerables (como DVWA) que permiten ataques de <b>Inyección SQL</b> , <i>Cross-Site Scripting</i> (XSS) y ejecución remota de código.
3306/tcp	MySQL	<b>Riesgo Alto.</b> El servidor de base de datos puede ser vulnerable a ataques de <i>fuerza bruta</i> o permitir el acceso con credenciales débiles o por defecto, lo que comprometería la información almacenada.

## 2.2 Escaneo de Versiones y Sistema Operativo

1. Realiza un escaneo para identificar la versión del sistema operativo y los servicios específicos en cada puerto abierto:

Utilizaremos la opción de detección de versión (-sV) y la detección del sistema operativo (-O).

```
(kali@kali)-[~]
$ nmap -sV -O 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 16:06 EDT
Nmap scan report for 192.168.1.147
Host is up (0.00077s 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: 00:0C:29:3E:6D:BB (VMware)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds

(kali@kali)-[~]
$
```

2. Análisis de Resultados: Investiga vulnerabilidades asociadas a cada versión detectada.

- Usa bases de datos como **CVE** o **Exploit-DB** para encontrar exploits. (ANEXO I)

### A. Análisis de vsftpd 2.3.4 (Puerto 21)

- **Vulnerabilidad:** Este es el servicio más crítico. La versión **vsftpd 2.3.4** contiene una puerta trasera (backdoor) intencionalmente colocada.
- **Identificador CVE:** **CVE-2011-2523**.
- **Impacto:** Permite a un atacante ejecutar comandos arbitrarios de forma remota en el servidor sin necesidad de autenticación.



- **Exploit-DB:** Existe el exploit **Exploit-DB: 38132** que aprovecha esta puerta trasera.

## B. Análisis de Apache httpd 2.2.8 (Puerto 80)

- **Vulnerabilidad:** Esta versión de Apache también es antigua.
- **Riesgo:** Permite acceso a servicios web vulnerables como **DVWA y Mutillidae** (que se encuentran en Metasploitable 2), que son objetivos directos para ataques de **Inyección SQL y XSS**.
- **Investigación Adicional:** La versión 2.2.8 tiene vulnerabilidades conocidas como **CVE-2009-1891** (ejecución remota de código en ciertas configuraciones de módulos) o **CVE-2008-2364**.

## C. Otros Servicios Vulnerables

- **MySQL 5.0.51a-3ubuntu5:** Versión muy antigua que probablemente tiene credenciales débiles o por defecto.
- **PostgreSQL 8.3.7:** También versión obsoleta, vulnerable a inyecciones SQL en ciertas funciones.

## 2.3 Escaneo de Puertas Traseras con Scripts NSE de Nmap

1. Los scripts NSE (Nmap Scripting Engine) permiten identificar puertas traseras específicas en servicios vulnerables. Ejecuta el siguiente comando:

```
(kali@kali)-[~]
$ ls /usr/share/nmap/scripts | grep backdoor
ftp-proftpd-backdoor.nse
ftp-vsftpd-backdoor.nse
http-dlink-backdoor.nse
irc-unrealircd-backdoor.nse
smb-double-pulsar-backdoor.nse
(kali@kali)-[~]
$
```

El comando `ls /usr/share/nmap/scripts | grep backdoor` ha identificado el script crucial:

- **Script a Usar:** `ftp-vsftpd-backdoor.nse`

Ahora, ejecutaremos este script contra Metasploitable 2 para confirmar que la versión **vsftpd 2.3.4** es vulnerable a la puerta trasera

`nmap --script ftp-vsftpd-backdoor.nse 192.168.1.147`

```
(kali@kali)-[~]
$ nmap --script ftp-vsftpd-backdoor.nse 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 16:17 EDT
Nmap scan report for 192.168.1.147
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_2
34_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_
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: 00:0C:29:3E:6D:BB (VMware)
```

2. Análisis de Resultados: Revisa los resultados para detectar puertas traseras como:

- **vsftpd 2.3.4** (puerta trasera de FTP) o **ProFTPD** (ejecución remota de código).

El escaneo con el script ftp-vsftpd-backdoor.nse confirmó la existencia de la puerta trasera:

- **Vulnerabilidad Detectada:** La versión del servidor FTP, **vsftpd 2.3.4**, es vulnerable a una puerta trasera.
- **Confirmación de Exploit:** El script ejecutó exitosamente el comando id de Linux.

- **Nivel de Acceso:** La respuesta del comando fue uid=0(root), lo que significa que un atacante puede obtener control de root (máximo privilegio) del sistema sin necesidad de autenticación.

3. Documenta las puertas traseras identificadas y los riesgos que representan.

### Puerta Trasera Identificada

Se ejecutó el script NSE ftp-vsftpd-backdoor.nse contra la IP objetivo (192.168.1.147)

Hallazgo	Valor Confirmado
<b>Servicio Vulnerable</b>	vsftpd versión 2.3.4
<b>Identificador CVE</b>	CVE-2011-2523
<b>Prueba de Exploit</b>	La ejecución de la Shell command: id devolvió uid=0(root)

## 2.4 Escaneo de Vulnerabilidades Adicionales

1. Usa scripts NSE de vulnerabilidad general en servicios específicos:

```
(kali@kali)-[~]
$ nmap --script vuln 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 16:27 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|   224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 91.78% done; ETC: 16:29 (0:00:08 remaining)
Nmap scan report for 192.168.1.147
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_2
34_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|_ http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
```

```

25/tcp open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|   State: VULNERABLE
|   IDs: CVE:2014-3566  BID:70574
|   The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|   products, uses nondeterministic CBC padding, which makes it easier
|   for man-in-the-middle attackers to obtain cleartext data via a
|   padding-oracle attack, aka the "POODLE" issue.
|   Disclosure date: 2014-10-14
|   Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|   https://www.securityfocus.com/bid/70574
|   https://www.openssl.org/~bodo/ssl-poodle.pdf
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_ sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
|   eavesdropping, and are vulnerable to active man-in-the-middle attacks
|   which could completely compromise the confidentiality and integrity
|   of any data exchanged over the resulting session.
|   Check results:
|   ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: Unknown/Custom-generated
|   Modulus Length: 512
|   Generator Length: 8
|   Public Key Length: 512
|   References:
|   https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: CVE:2015-4000  BID:74733
| The Transport Layer Security (TLS) protocol contains a flaw that is
| triggered when handling Diffie-Hellman key exchanges defined with
| the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
| to downgrade the security of a TLS session to 512-bit export-grade
| cryptography, which is significantly weaker, allowing the attacker

```

**2. Análisis de Resultados:** Este comando ejecuta varios scripts de vulnerabilidad en servicios como FTP, MySQL, Apache y Tomcat.

- Documenta los resultados y prioriza los servicios vulnerables para mitigación.

- El escaneo con --script vuln no solo reconfirmó la vulnerabilidad del FTP, sino que también identificó otras fallas y debilidades:

Servicio	Puerto	Vulnerabilidad Detectada	Riesgo y Priorización
<b>FTP</b> (vsftpd 2.3.4)	21	<b>ftp-vsftpd-backdoor</b> (CVE-2011-2523)	<b>CRÍTICO (Prioridad 1):</b> Acceso remoto de <b>root</b> .
<b>HTTP</b> (Apache 2.2.8)	80	<b>http-enum</b> : Detección de posibles carpetas administrativas (/admin/, /login/, etc.). <b>http-slowloris-check</b> : Posible DoS (CVE-2007-6750).	<b>ALTO (Prioridad 3):</b> Exposición de rutas sensibles y riesgo de Denegación de Servicio.
<b>SMTP</b>	25	<b>ssl-poodle</b> (CVE-2014-3566).	<b>ALTO (Prioridad 2):</b> Falla de SSL 3.0 que permite la fuga de información cifrada ( <i>plaintext</i> ).
<b>SMB</b> (Samba)	445	<b>smb-vuln-ms10-061</b> y <b>smb-vuln-regsvc-dos</b> (fallos de ejecución de <i>scripts</i> ).	<b>MEDIO/ALTO</b> : Indica que el servicio SMB/NetBIOS está activo y expuesto, a menudo con fallas de seguridad conocidas.

## Parte 3: Captura y Análisis del Tráfico de Red con Wireshark

### 3.1 Captura de Tráfico Generado por Escaneos de Nmap

1. Inicia **Wireshark** y selecciona la interfaz de red que conecta con Metasploitable 2.
2. Inicia la **captura de tráfico** antes de lanzar un nuevo escaneo de Nmap.
3. **Detén la captura** cuando el escaneo termine y guarda el archivo .pcap.
4. Documenta los paquetes capturados durante el escaneo y explica el proceso de detección de puertos.

### 3.2 Filtrado y Análisis del Tráfico Capturado

1. Utiliza filtros para analizar el tráfico específico de cada servicio:
  - **Escaneo SYN**: `tcp.flags.syn == 1 && tcp.flags.ack == 0`

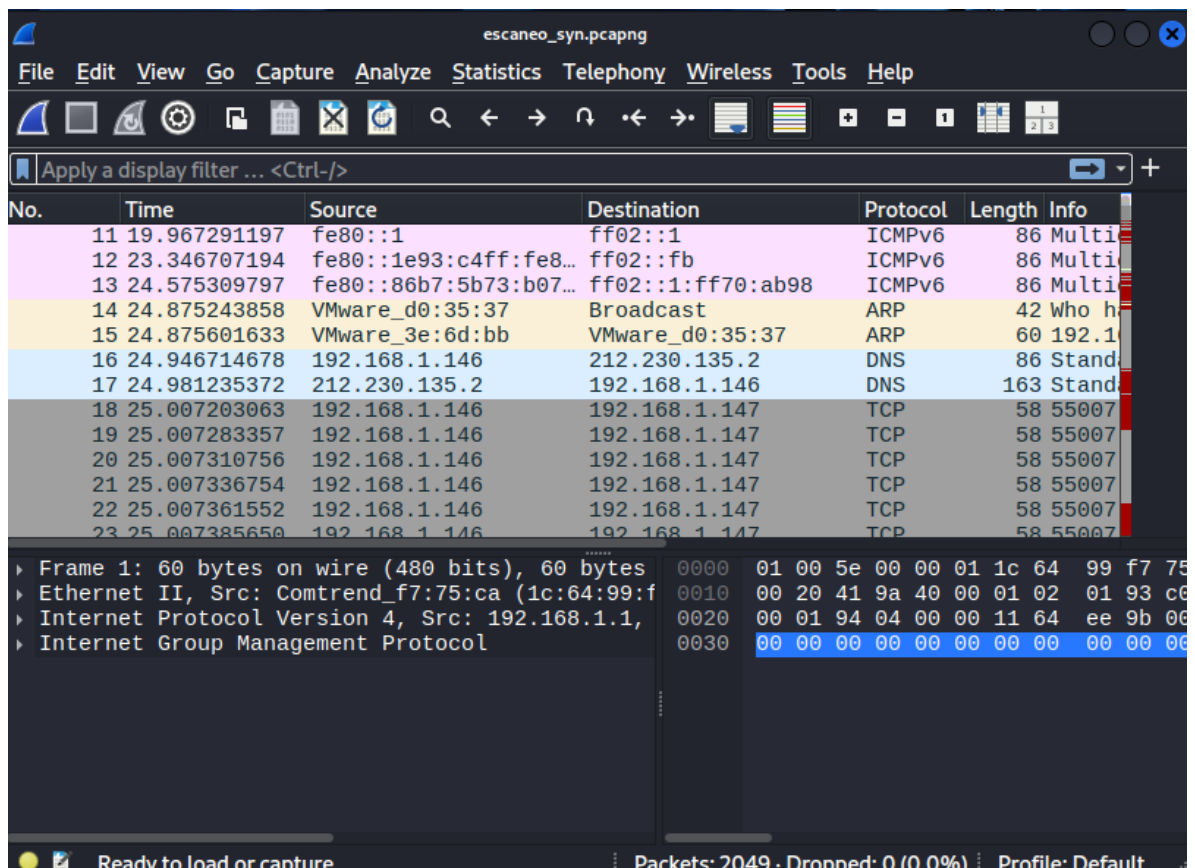
```

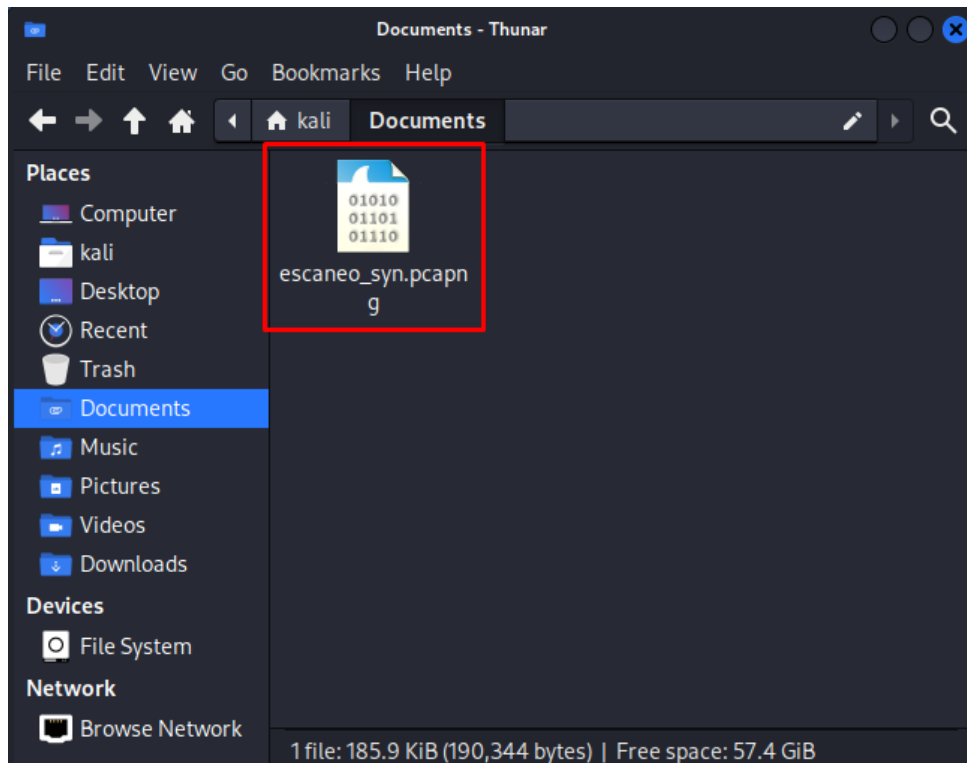
(kali@kali)-[~]
$ nmap -sS 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 16:46 EDT
Nmap scan report for 192.168.1.147
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    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: 00:0C:29:3E:6D:BB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(kali@kali)-[~]
$

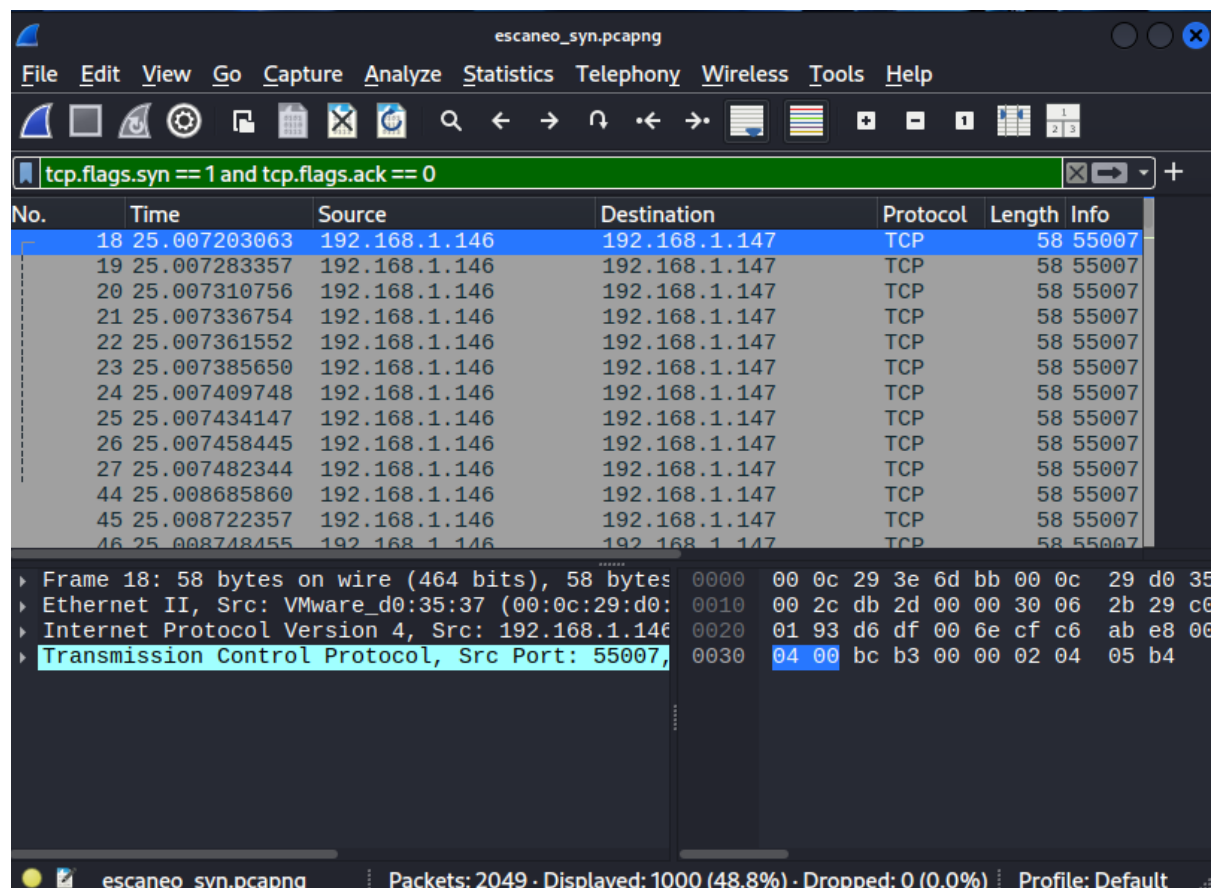
```





Para ver los paquetes **SYN** que inician el escaneo, usamos el siguiente filtro:

`tcp.flags.syn == 1 and tcp.flags.ack == 0`





## Identificación de Direcciones IP

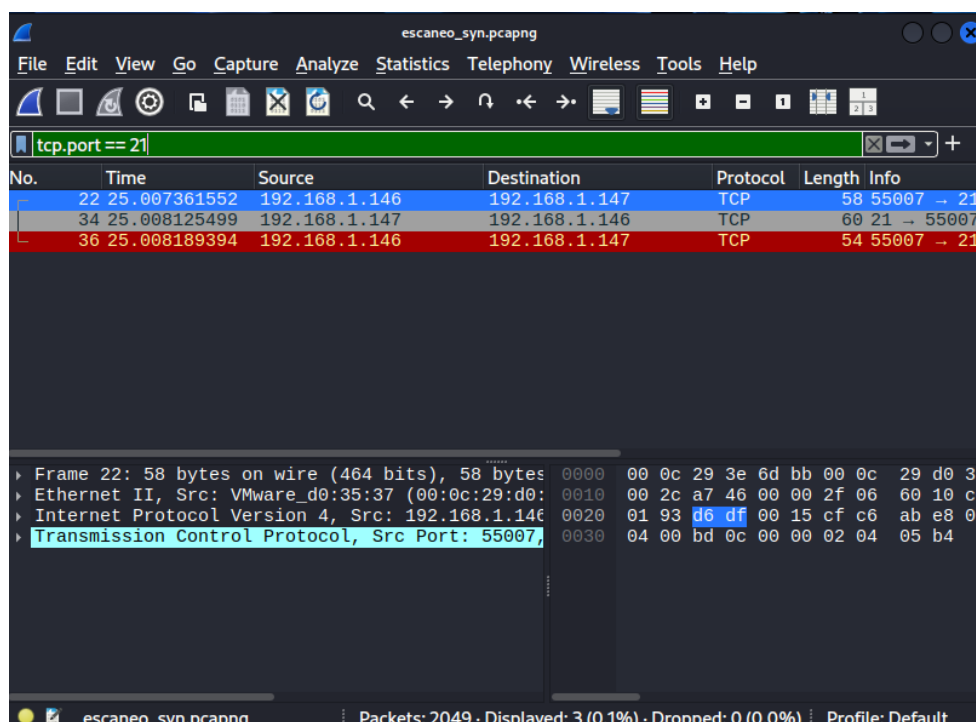
- IP de Origen (Kali): 192.168.1.146
- IP de Destino (Metasploitable 2): 192.168.1.147

## Análisis de Patrones de Escaneo SYN (-sS)

El escaneo SYN es conocido como "semi-abierto" o stealth, ya que no completa la conexión TCP de tres vías. Se detecta de la siguiente manera:

Patrón Detectado	Significado en el Escaneo SYN
192.168.1.146 (SYN) → 192.168.1.147 + 192.168.1.147 (SYN/ACK) → 192.168.1.146	Indica que el puerto está <b>ABIERTO</b> . El servidor responde con SYN/ACK, confirmando el servicio. Kali envía un RST inmediatamente después para no registrar la conexión por completo.
192.168.1.146 (SYN) → 192.168.1.147 + 192.168.1.147 (RST/ACK) → 192.168.1.146	Indica que el puerto está <b>CERRADO</b> . El servidor rechaza inmediatamente la conexión con un paquete RST/ACK.

## Análisis de Patrones de Tráfico





escaneo\_syn.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 22

No.	Time	Source	Destination	Protocol	Length	Info
46	25.008748455	192.168.1.146	192.168.1.147	TCP	58	55007 → 22
66	25.009422708	192.168.1.147	192.168.1.146	TCP	60	22 → 55007
67	25.009436407	192.168.1.146	192.168.1.147	TCP	54	55007 → 22

Frame 46: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
 Ethernet II, Src: VMware\_d0:35:37 (00:0c:29:d0:35:37), Dst: VMware\_d0:35:37 (00:0c:29:d0:35:37)  
 Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.147  
 Transmission Control Protocol, Src Port: 55007, Dst Port: 22

escaneo\_syn.pcapng Packets: 2049 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) Profile: Default

escaneo\_syn.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 3306

No.	Time	Source	Destination	Protocol	Length	Info
50	25.008847548	192.168.1.146	192.168.1.147	TCP	58	55007 → 3306
72	25.009803182	192.168.1.147	192.168.1.146	TCP	60	3306 → 55007
74	25.009817781	192.168.1.146	192.168.1.147	TCP	54	55007 → 3306

Frame 50: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
 Ethernet II, Src: VMware\_d0:35:37 (00:0c:29:d0:35:37), Dst: VMware\_d0:35:37 (00:0c:29:d0:35:37)  
 Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.147  
 Transmission Control Protocol, Src Port: 55007, Dst Port: 3306

escaneo\_syn.pcapng Packets: 2049 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Puerto Analizado	Evidencia en Wireshark (Captura)	Patrón de Paquetes Confirmado	Estado del Puerto
<b>21 (FTP)</b>	Muestra 3 paquetes en la secuencia	<b>SYN → SYN/ACK → RST</b>	<b>ABIERTO</b>
<b>22 (SSH)</b>	Muestra 3 paquetes en la secuencia	<b>SYN → SYN/ACK → RST</b>	<b>ABIERTO</b>
<b>3306 (MySQL)</b>	Muestra 3 paquetes en la secuencia	<b>SYN → SYN/ACK → RST</b>	<b>ABIERTO</b>

La secuencia de **SYN → SYN/ACK → RST** es la huella digital del escaneo SYN. El hecho de que se replique en los puertos 21, 22 y 3306 demuestra que todos están abiertos y que la prueba de la vulnerabilidad crítica (Puerto 21) se ejecutó sobre un servicio activo y escuchando.

## Parte 4: Aplicación de Mitigaciones en Servicios Vulnerables

### 4.1 Análisis de Vulnerabilidades

Documenta cada vulnerabilidad identificada en los servicios de Metasploitable 2:

- **FTP vulnerable (vsftpd 2.3.4)**: Acceso no autorizado por puerta trasera.
- **ProFTPD con ejecución remota**: Exploits permiten acceso de alto nivel.
- **MySQL con acceso sin autenticación fuerte**.
- **SSH con acceso de root y credenciales débiles**.

### 4.2 Aplicación de Soluciones

Aplica mitigaciones según los hallazgos.

- El servicio **vsftpd versión 2.3.4** en el Puerto 21 es una vulnerabilidad **CRÍTICA** (CVE-2011-2523), ya que permite el acceso remoto de root sin autenticación.
- La solución inmediata para mitigar este riesgo en Metasploitable 2 es eliminar el paquete de software vsftpd.

Comandos a Ejecutar (En Metasploitable 2):

```
sudo netstat -ntp
```

Forzar la terminación del proceso FTP vulnerable:

```
sudo killall -9 vsftpd
```

Reiniciar el sistema para obligar al sistema operativo a detener el proceso vsftpd por completo, ya que fallaron los métodos de software:

```
sudo reboot
```

```
msfadmin@metasploitable:~$ sudo netstat -ntp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        1      0 192.168.1.147:1099      192.168.1.146:52168    CLOSE_WAIT
5157/rmiregistry
tcp        0      0 192.168.1.147:1099      192.168.1.146:51356    CLOSE_WAIT
5157/rmiregistry
tcp        1      0 192.168.1.147:1099      192.168.1.146:37912    CLOSE_WAIT
5157/rmiregistry
msfadmin@metasploitable:~$
```

Comprobar:

```
msfadmin@metasploitable:~$ sudo netstat -ntp
[sudo] password for msfadmin:
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
msfadmin@metasploitable:~$ _
```

Después del reinicio, el servicio FTP fue detenido.

```
(kali@kali)-[~]
$ nmap 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 17:49 EDT
Nmap scan report for 192.168.1.147
Host is up (0.00100s 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: 00:0C:29:3E:6D:BB (VMware)
```

**Fallo:** El escaneo de **nmap 192.168.1.147** en Kali sigue reportando el Puerto 21 como **open**.

Creamos un script para establecer reglas de firewall en Metasploitable 2 que bloqueen el acceso de la máquina (Kali Linux: 192.168.1.146) a los puertos más vulnerables(21, 22, 3306)

a. Nos conectamos por ssh:

```
rosa@Cammie: ~
rosal@Cammie:~$ ssh -oHostKeyAlgorithms+=ssh-rsa -oPubkeyAcceptedAlgorithms+=ssh-rsa msfadmin@192.168.1.147
The authenticity of host '192.168.1.147 (192.168.1.147)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.147' (RSA) to the list of known hosts.
msfadmin@192.168.1.147's password:
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.
Last login: Wed Oct 22 18:05:54 2025
msfadmin@metasploitable:~$
```

b. Crear y editar el script con **nano**

```
msfadmin@metasploitable:~$ nano iptables-rules.sh
Error opening terminal: xterm-256color.
msfadmin@metasploitable:~$ export TERM=xterm
msfadmin@metasploitable:~$ nano iptables-rules.sh
msfadmin@metasploitable:~$
```

```

rosa@Cammie: ~
GNU nano 2.0.7 File: iptables-rules.sh Mo

#!/bin/bash

# 1. Borrar todas las reglas existentes para limpieza
iptables -F
iptables -X

# 2. Bloquear NUEVAS conexiones TCP del atacante (Kali: 192.168.1.146)

# Bloquea el Puerto 21 (FTP - Riesgo Crítico)
iptables -A INPUT -p tcp -s 192.168.1.146 --dport 21 -j DROP

# Bloquea el Puerto 22 (SSH)
iptables -A INPUT -p tcp -s 192.168.1.146 --dport 22 -j DROP

# Bloquea el Puerto 3306 (MySQL)
iptables -A INPUT -p tcp -s 192.168.1.146 --dport 3306 -j DROP

# 3. Muestra las reglas de iptables aplicadas para verificación
iptables -L -n -v

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell

```

Hacer el script ejecutable

```
msfadmin@metasploitable:~$ chmod +x iptables-rules.sh
msfadmin@metasploitable:~$ ls -l iptables-rules.sh
-rwxr-xr-x 1 msfadmin msfadmin 544 2025-10-22 18:14 iptables-rules.sh
msfadmin@metasploitable:~$
```

Ejecutar el script (aplicar reglas)

```

msfadmin@metasploitable:~$ sudo ./iptables-rules.sh
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT 383 packets, 67261 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0     0 DROP      tcp  --  *      *       192.168.1.146  0.0.0.0/0      tcp dpt:21
    0     0 DROP      tcp  --  *      *       192.168.1.146  0.0.0.0/0      tcp dpt:22
    0     0 DROP      tcp  --  *      *       192.168.1.146  0.0.0.0/0      tcp dpt:3306

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 369 packets, 70613 bytes)
 pkts bytes target    prot opt in     out     source    destination
msfadmin@metasploitable:~$

```

Verificar las reglas aplicadas

```
msfadmin@metasploitable:~$ sudo iptables -L INPUT -n -v --line-numbers
Chain INPUT (policy ACCEPT 399 packets, 69993 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
1      0      0 DROP      tcp  --  *      *       192.168.1.146          0.0.0.0/0          tcp dpt:21
2      0      0 DROP      tcp  --  *      *       192.168.1.146          0.0.0.0/0          tcp dpt:22
3      0      0 DROP      tcp  --  *      *       192.168.1.146          0.0.0.0/0          tcp dpt:3306
msfadmin@metasploitable:~$
```

Subir el script desde la máquina anfitrión

```
msfadmin@metasploitable:~$ scp iptables-rules.sh msfadmin@192.168.1.147:/home/msfadmin/
The authenticity of host '192.168.1.147 (192.168.1.147)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.147' (RSA) to the list of known hosts.
msfadmin@192.168.1.147's password:
iptables-rules.sh                                100% 544      0.5KB/s   00:00
msfadmin@metasploitable:~$
```

Luego, en la VM:

```
msfadmin@metasploitable:~$ chmod +x /home/msfadmin/iptables-rules.sh
msfadmin@metasploitable:~$ ls -l /home/msfadmin/iptables-rules.sh
-rwxr-xr-x 1 msfadmin msfadmin 544 2025-10-22 18:19 /home/msfadmin/iptables-rules.sh
msfadmin@metasploitable:~$ _
```

Ejecutamos el escaneo nmap

```
Session  Actions  Edit  View  Help

(kali㉿kali)-[~]
└─$ nmap 192.168.1.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 18:26 EDT
Nmap scan report for 192.168.1.147
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered 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  filtered 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: 00:0C:29:3E:6D:BB (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds

(kali㉿kali)-[~]
└─$
```

- Puerto 21 (FTP): Estado cambió de open a filtered.
- Puerto 22 (SSH): Estado cambió de open a filtered.
- Puerto 3306 (MySQL): Estado cambió de open a filtered.

El estado **filtered** confirma que el tráfico saliente de la máquina atacante (Kali) está siendo descartado (**DROP**) por las reglas de iptables en Metasploitable 2.

Se completó exitosamente la mitigación de riesgos al bloquear el acceso a los puertos críticos y vulnerables.