

LABORATORIO DE PENTESTING - METASPLOITABLE 2

Reto:  4

Estudiante: Roberto Flores Segundo (Siegfried_FS) 


Instructora: Karla Andrea Najera Noyola (l1ttl3bugc4t) 

Institución: Purplespace Academy & Hacktitud 

Fecha: 22-Septiembre-2025  17








IP Objetivo: 192.168.1.68

OBJETIVO: Mapeando la Ciber-Fortaleza

Nuestra misión fue simple: sumergirnos en la máquina **Metasploitable 2**  para descubrir sus secretos (y vulnerabilidades) usando nuestro arsenal de reconocimiento activo. El objetivo principal era mapear la superficie de ataque, identificar servicios clave y encontrar los puntos de entrada antes de un ataque.

METODOLOGÍA Y HERRAMIENTAS

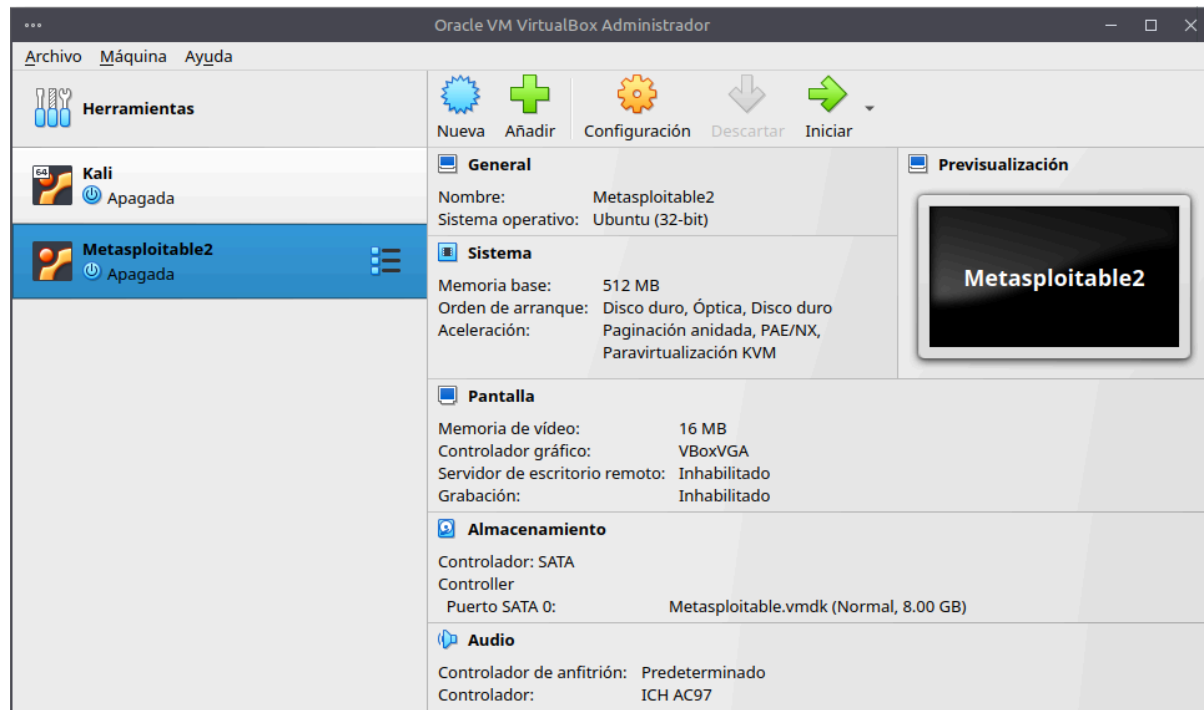
Para esta operación de reconocimiento, nos equipamos con el arsenal esencial de un hacker ético.

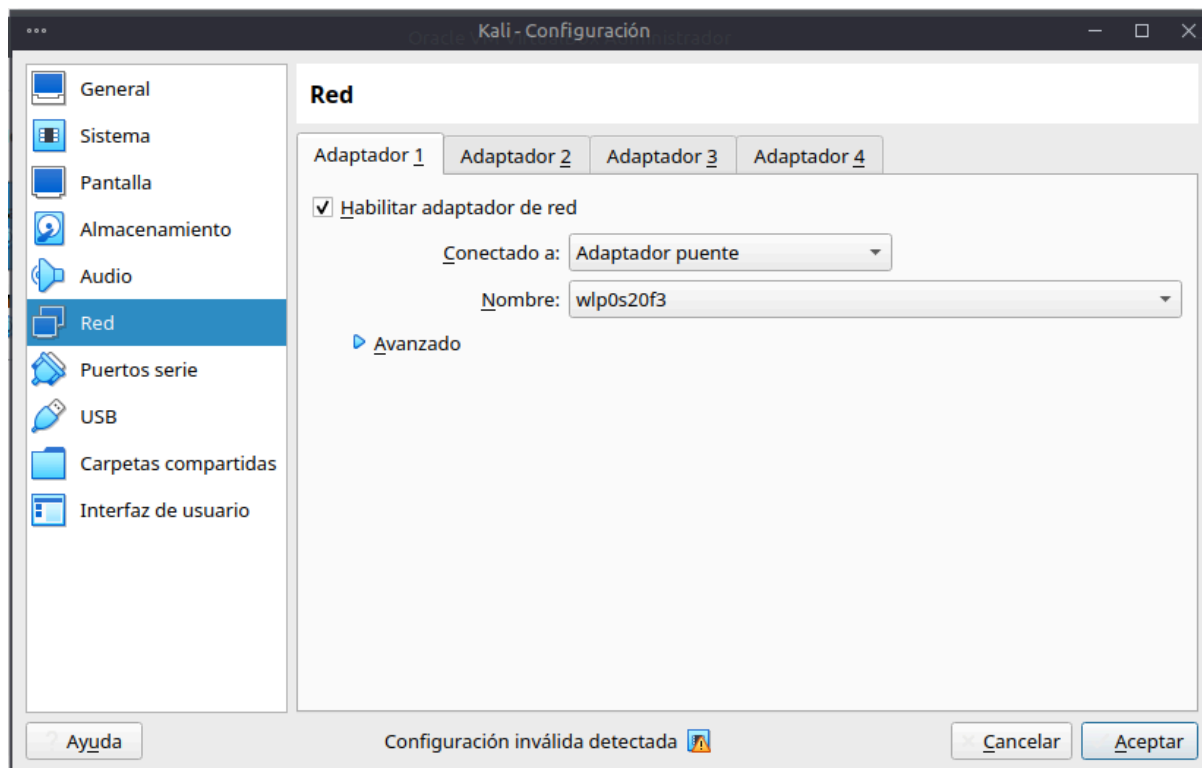
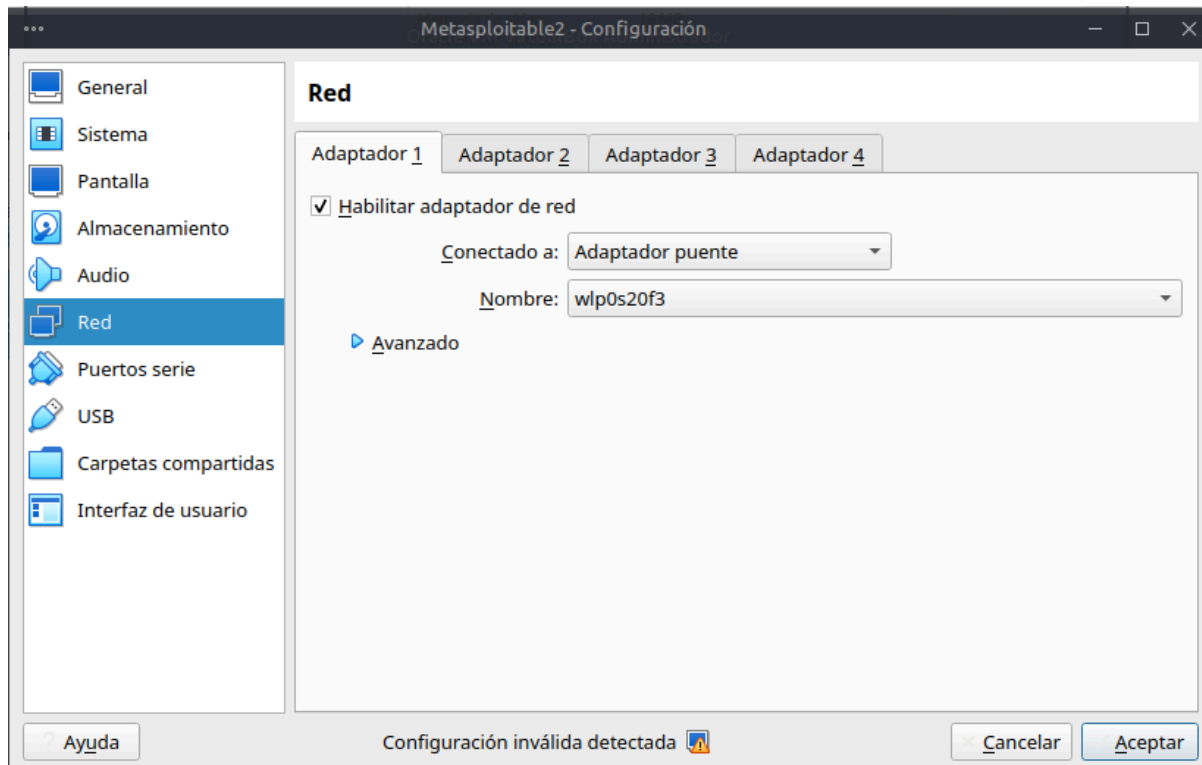
Herramienta 	Propósito 
VirtualBox	Nuestro campo de entrenamiento virtual  .
Kali Linux	La navaja suiza del hacker ético  .
Metasploitable 2	La caja de sorpresas (¡y vulnerabilidades!)  .
nmap	Nuestro radar de servicios y puertos  .
Enumeración Manual	La mirada de detective para detalles que las herramientas pierden  .

DESARROLLO DE ACTIVIDADES

1. Instalación y Configuración del Laboratorio

La víctima, Metasploitable 2, fue desplegada con éxito en **VirtualBox**. Con 512MB de RAM y un disco duro virtual de 8GB, el sistema estaba listo para la evaluación. Ambas máquinas, Kali Linux y Metasploitable 2, fueron conectadas en **modo puente**, permitiendo una comunicación directa en nuestra red local.



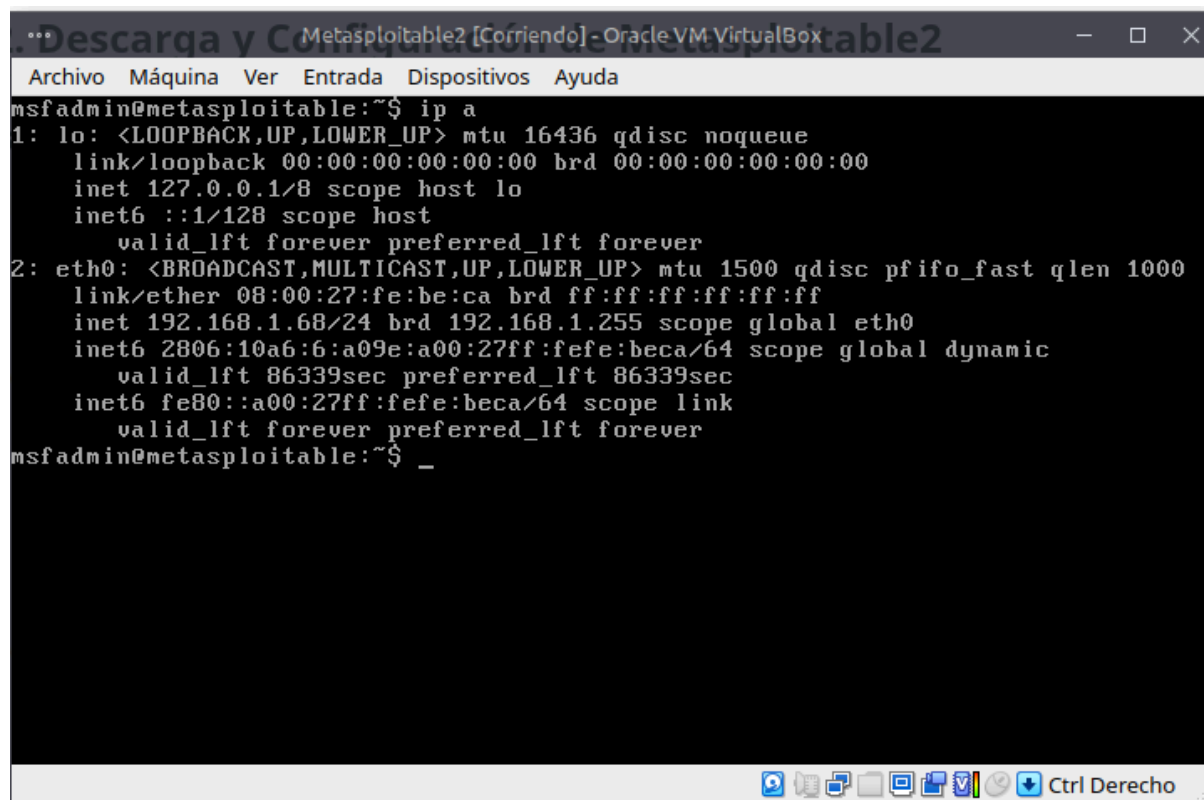


2. Obtención de IP y Escaneo de Puertos

Con las credenciales por defecto (msfadmin:msfadmin), accedimos al equipo objetivo y

ejecutamos el comando ip a para obtener su dirección de red.

IP obtenida: 192.168.1.68



```
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 08:00:27:fe:be:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.68/24 brd 192.168.1.255 scope global eth0
    inet6 2806:10a6:6:a09e:a00:27ff:fefe:beca/64 scope global dynamic
        valid_lft 86339sec preferred_lft 86339sec
    inet6 fe80::a00:27ff:fefe:beca/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Posteriormente, lanzamos un escaneo exhaustivo con nmap para identificar todos los puertos abiertos y sus servicios correspondientes.

Comando ejecutado: nmap -sS -sV -vvv -p- 192.168.1.68

El resultado fue una mina de oro: **29 servicios abiertos**, lo que representa una superficie de ataque increíblemente amplia.

metasploitable2_scan_20250922_075341.txt

ENUMERACIÓN DETALLADA DE SERVICIOS

SERVICIO 1: FTP (Puerto 21) - vsftpd 2.3.4

- **Acceso:** Logramos un acceso exitoso usando las credenciales por defecto, msfadmin:msfadmin.
- **Hallazgos:** Dentro del directorio /home/msfadmin, encontramos archivos potencialmente sensibles, como .mysql_history y .sudo_as_admin_successful.
- **Análisis de Vulnerabilidad:** La versión **vsftpd 2.3.4** contiene un **backdoor** conocido

(CVE-2011-2523), lo que representa un riesgo crítico.

Evidencia:

```
(kali@kali)~$ ftp 192.168.1.68
Connected to 192.168.1.68.
220 (vsFTPD 2.3.4)
Name (192.168.1.68:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6617|).
150 Here comes the directory listing.
drwxr-xr-x  6 1000    1000      4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> pwd
Remote directory: /home/msfadmin
ftp> dir -la
229 Entering Extended Passive Mode (|||27274|).
150 Here comes the directory listing.
drwxr-xr-x  5 1000    1000      4096 May 20  2012 .
drwxr-xr-x  6 0        0        4096 Apr 16  2010 ..
lrwxrwxrwx  1 0        0         9 May 14  2012 .bash_history -> /dev/null
drwxr-xr-x  4 1000    1000      4096 Apr 17  2010 .distcc
-rw-----  1 0        0        4174 May 14  2012 .mysql_history
-rw-r--r--  1 1000    1000      586 Mar 16  2010 .profile
-rwx-----  1 1000    1000      4 May 20  2012 .rhosts
drwx-----  2 1000    1000      4096 May 18  2010 .ssh
-rw-r--r--  1 1000    1000      0 May 07  2010 .sudo_as_admin_successful
drwxr-xr-x  6 1000    1000      4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> █
```

SERVICIO 2: SMB (Puerto 445) - Samba 3.X

- **Acceso:** Un intento de conexión anónima (`smbclient -L 192.168.1.68 -N`) fue exitoso. ¡Samba nos dio la bienvenida sin credenciales!
- **Hallazgos:** Se encontraron recursos compartidos como `print$`, `tmp` (con el comentario "oh noes!") e `IPC$`. El directorio `/tmp` es accesible para lectura y escritura, lo que representa un punto de entrada fácil.
- **Análisis de Vulnerabilidad:** La versión Samba 3.0.20-Debian es vulnerable a múltiples CVEs, y el acceso anónimo agrava la situación.

Evidencia:

```

(kali㉿kali)-[~]
$ smbclient //192.168.1.68/opt -N
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

(kali㉿kali)-[~]
$ smbclient //192.168.1.68/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0  Mon Sep 22 08:20:45 2025
..              DR          0  Sun May 20 13:36:12 2012
.ICE-unix        DH          0  Mon Sep 22 01:46:48 2025
.X11-unix        DH          0  Mon Sep 22 01:46:52 2025
4795.jsvc_up     R           0  Mon Sep 22 01:46:58 2025
.X0-lock        HR          11 Mon Sep 22 01:46:52 2025

7282168 blocks of size 1024. 5437840 blocks available
smb: \> dir
.                D           0  Mon Sep 22 08:20:45 2025
..              DR          0  Sun May 20 13:36:12 2012
.ICE-unix        DH          0  Mon Sep 22 01:46:48 2025
.X11-unix        DH          0  Mon Sep 22 01:46:52 2025
4795.jsvc_up     R           0  Mon Sep 22 01:46:58 2025
.X0-lock        HR          11 Mon Sep 22 01:46:52 2025

7282168 blocks of size 1024. 5437840 blocks available
smb: \> pwd
Current directory is \\192.168.1.68\tmp\

```

SERVICIO 3: HTTP (Puerto 80) - Apache 2.2.8

- **Acceso:** Este servicio nos dio una sorpresa. Aunque el escaneo inicial con nmap lo reportó como abierto, un intento de verificación posterior con curl falló.
- **Análisis de Vulnerabilidad:** Este comportamiento inconsistente podría ser un indicio de un servicio inestable o de un mecanismo de protección activo que bloquea múltiples conexiones. Este hallazgo merece una investigación más a fondo.

Evidencia:

```
(kali㉿kali)-[~]
└─$ nmap --script http-* 192.168.1.68 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 08:22 CST
Pre-scan script results:
|_http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtext's API. See https://www.rob
tex.com/api/
Nmap scan report for 192.168.1.68
Host is up (0.00027s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 08:00:27:FE:BE:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

(kali㉿kali)-[~]
└─$
```

🧠 CONCLUSIONES Y LECCIONES APRENDIDAS

Este laboratorio de pentesting fue un recordatorio poderoso de la importancia de la higiene digital. Metasploitable 2 es una plataforma perfecta que demuestra cómo las configuraciones por defecto y el software obsoleto pueden dejar un sistema completamente expuesto.

	Aspectos Técnicos 🛠️	Aspectos Metodológicos 📝
✅ Lo Logrado	La combinación de escaneos automáticos (nmap) y la enumeración manual fue crucial para encontrar vulnerabilidades.	La documentación sistemática de cada paso del proceso es fundamental para el análisis posterior y la generación de un reporte completo.
💡 Lecciones	Las credenciales por defecto son el eslabón más débil. Se deben cambiar de inmediato. La existencia de múltiples servicios innecesarios aumenta drásticamente la superficie de ataque.	La verificación cruzada (como la prueba del puerto 80) es vital para aumentar la confiabilidad de los hallazgos y detectar anomalías.

Recomendaciones:

- **Cambiar credenciales por defecto:** Es el paso de seguridad más básico y el primero que debe implementarse.
- **Actualizar software:** Actualizar o parchar servicios como vsftpd y Samba para mitigar vulnerabilidades conocidas.

- **Desactivar servicios no esenciales:** Cierre los puertos que no son necesarios, como Telnet o el **bindshell** del puerto 1524, para reducir la superficie de ataque.

Happy Hacking! - Siegfried_FS 