WEB2S SECURITY

Reporte de pentesting y comprobación de vulnerabilidades, utilizando Metaesploitable2 y Kali Linux.

Web2S Security
Febrero 2024
versión 1.0

Realizado por: Miguel Ángel Fernández Parejo
mafparejo@proton.me
mder716@gmail.com
mafparejo@gmail.com

CONTENIDO

1 AUTORÍA DEL DOCUMENTO Y DERECHOS DE COPYRIGHT

El presente documento ha sido realizado por Web2S Security, y está

CLIENTE: Oblibion, S.A.
PROYECTO: Seguridad y pentesting.
CLASIFICACIÓN: Confidencial
AUTOR: Miguel Ángel Fernández Parejo

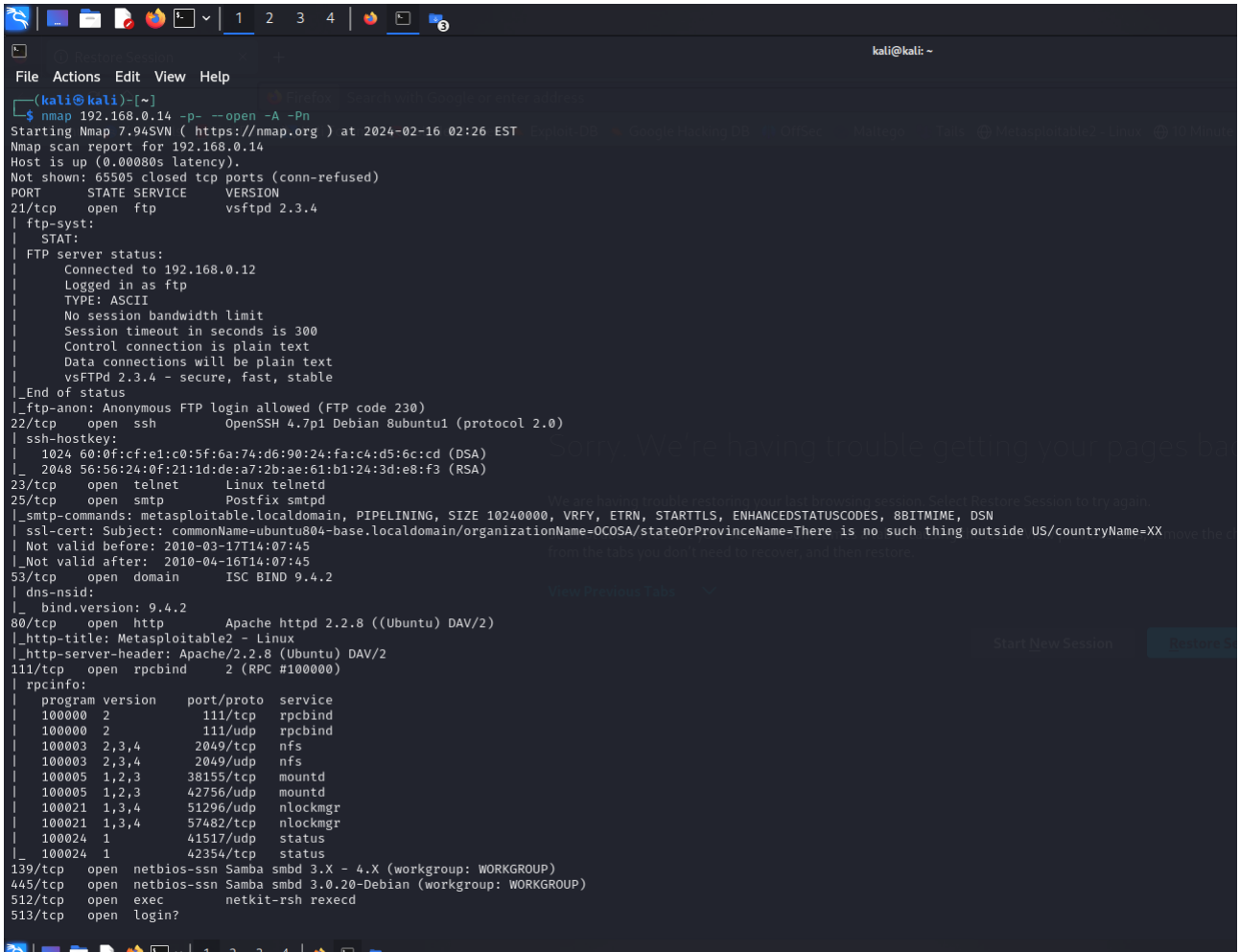
2 ÁMBITO Y ALCANCE DE LA AUDITORÍA

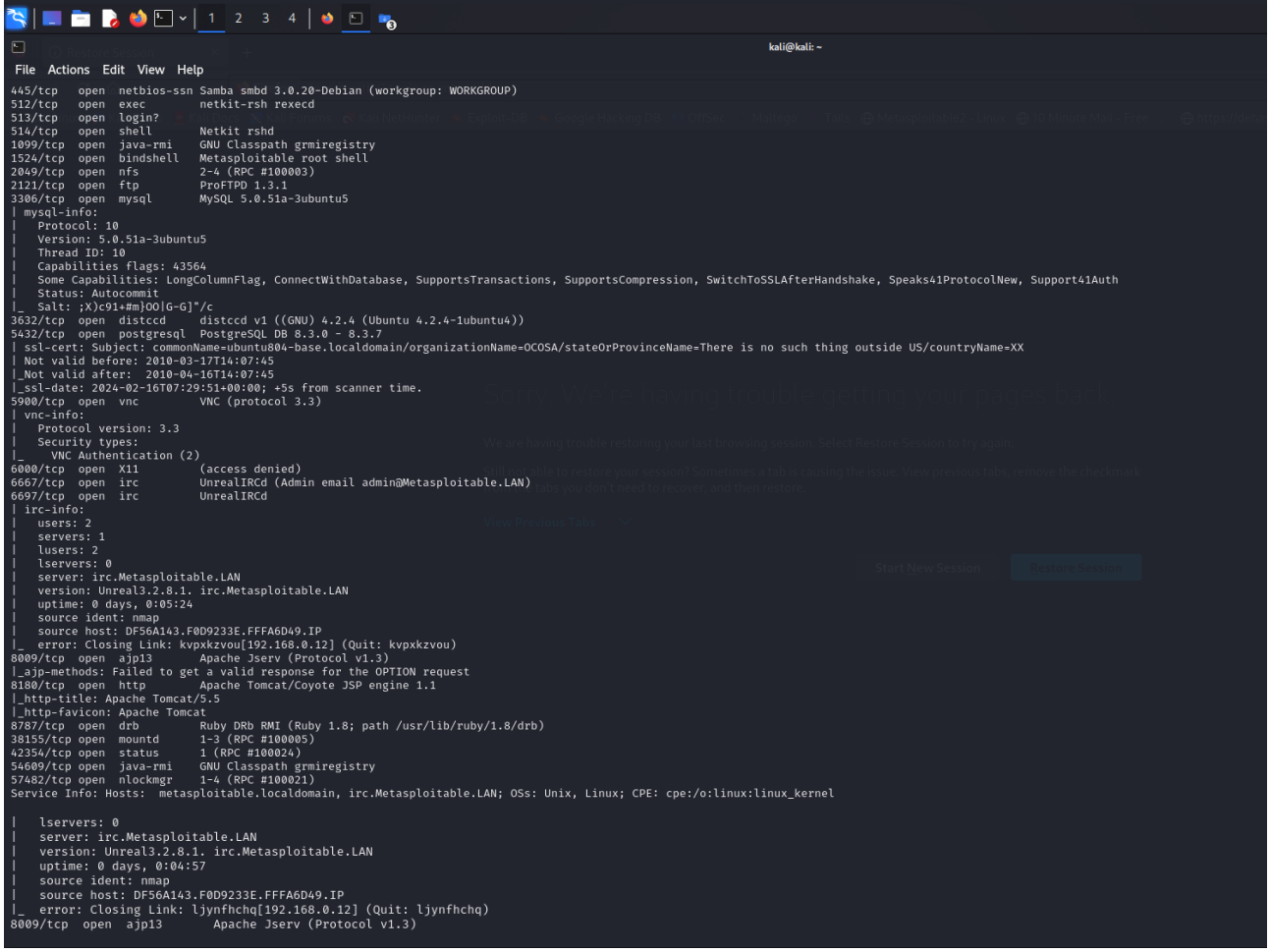
Se ha hecho un análisis de infraestructura y análisis de vulnerabilidades.

2.1 ANÁLISIS DE INFRAESTRUCTURA

La auditoría se ha realizado en Metaesploitable2 y Kali Linux, utilizando la herramienta Nmap, se han recuperado los siguientes datos:

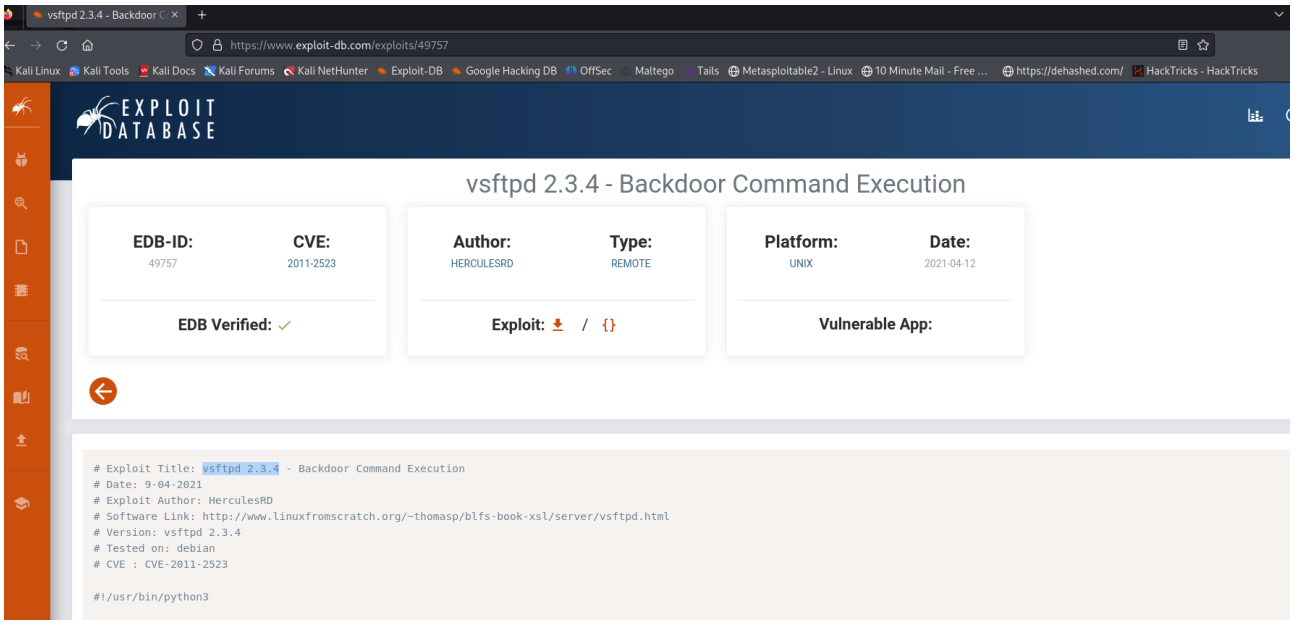
Escaneando la IP de Meta http://192.168.0.14 con nmap lanza estos resultados:


1 2 3 4
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.14 -p- --open -A -Pn
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-16 02:26 EST
Nmap scan report for 192.168.0.14
Host is up (0.00080s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.0.12
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 38155/tcp mountd
| 100005 1,2,3 42756/udp mountd
| 100021 1,3,4 51296/udp nlockmgr
| 100021 1,3,4 57482/tcp nlockmgr
| 100024 1 41517/udp status
|_ 100024 1 42354/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?


1 2 3 4
kali@kali: ~
File Actions Edit View Help
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 10
| Capabilities flags: 43564
| Some Capabilities: LongColumnFlag, ConnectWithDatabase, SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, Support41Auth
| Status: Autocommit
|_ Salt: ;X)c91+#m}OO|G-G]"/c
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2024-02-16T07:29:51+00:00; +5s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp open irc UnrealIRCd
| irc-info:
| users: 2
| servers: 1
| lusers: 2
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:05:24
| source ident: nmap
| source host: DF56A143.F0D9233E.FFFA6D49.IP
|_ error: Closing Link: kvpxkzvou[192.168.0.12] (Quit: kvpxkzvou)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38155/tcp open mountd 1-3 (RPC #100005)
42354/tcp open status 1 (RPC #100024)
54609/tcp open java-rmi GNU Classpath grmiregistry
57482/tcp open nlockmgr 1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:04:57
| source ident: nmap
| source host: DF56A143.F0D9233E.FFFA6D49.IP
|_ error: Closing Link: ljynfhchq[192.168.0.12] (Quit: ljynfhchq)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

Vamos a ir buscando vulnerabilidades a través de los puertos abiertos, con sus versiones, para ello copiamos por ej. el primero y vamos buscar en Google, las vulnerabilidades:
vsftpd 2.3.4

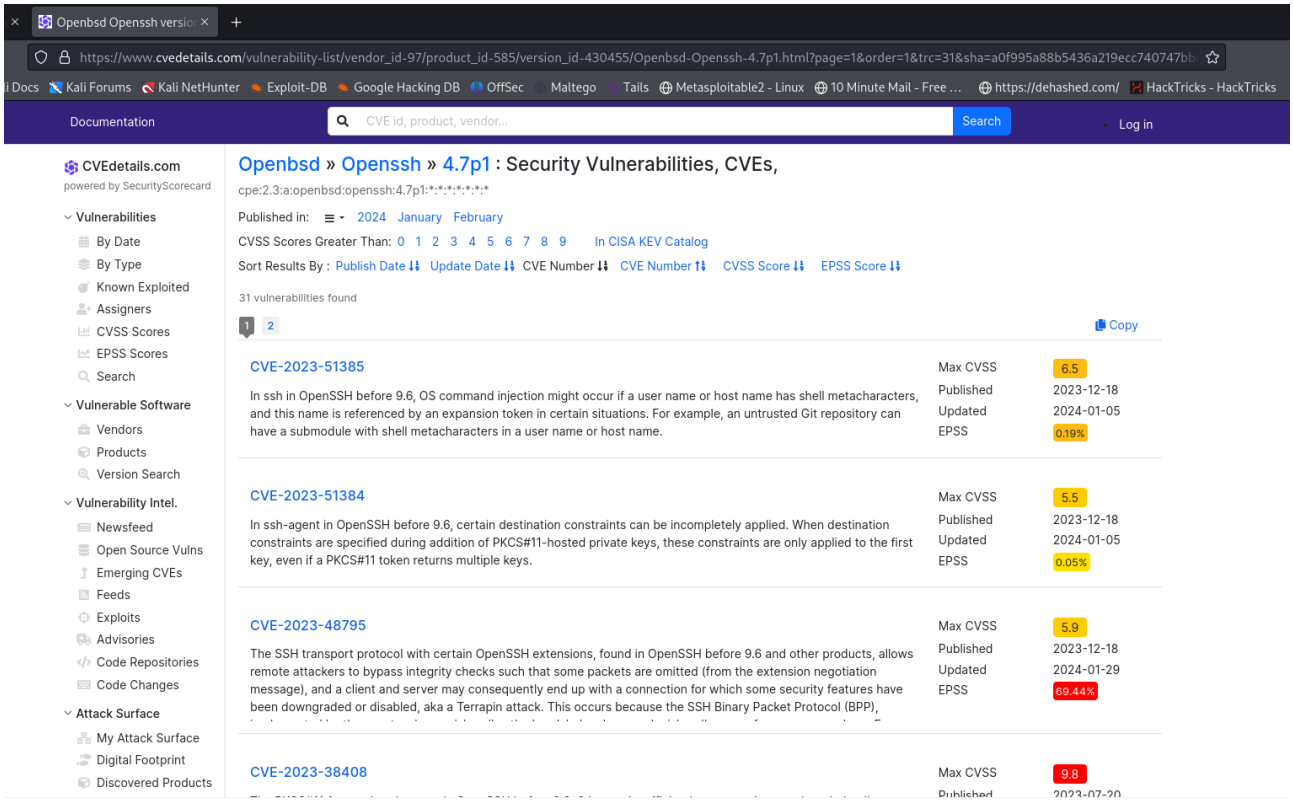
En la web exploit-db.com encontramos este exploit que se lanza en python3:



Siguiente servicio/puerto OpenSSH 4.7.p1:

```
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Buscamos en Google algún exploit, en cvedetails.com encontramos muchas vulnerabilidades:

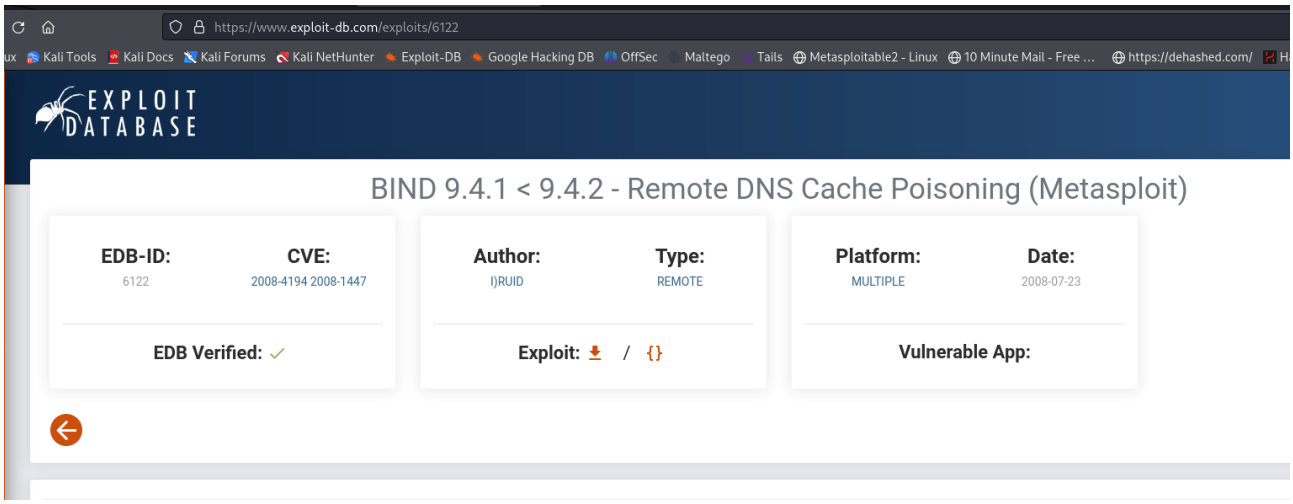


El OpenSSH 4.7.p1 al ser una versión antigua se aconseja actualización de este servicio.

Buscamos en Google vulnerabilidades para el servicio ISC BIND 9.4.2

```
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPE
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
```

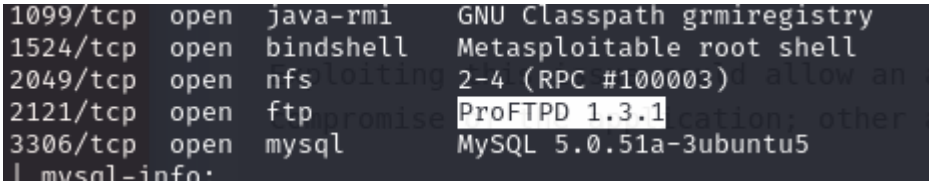
En exploit-db.com, nos dice que tiene un envenenamiento de caché remoto por DNS:



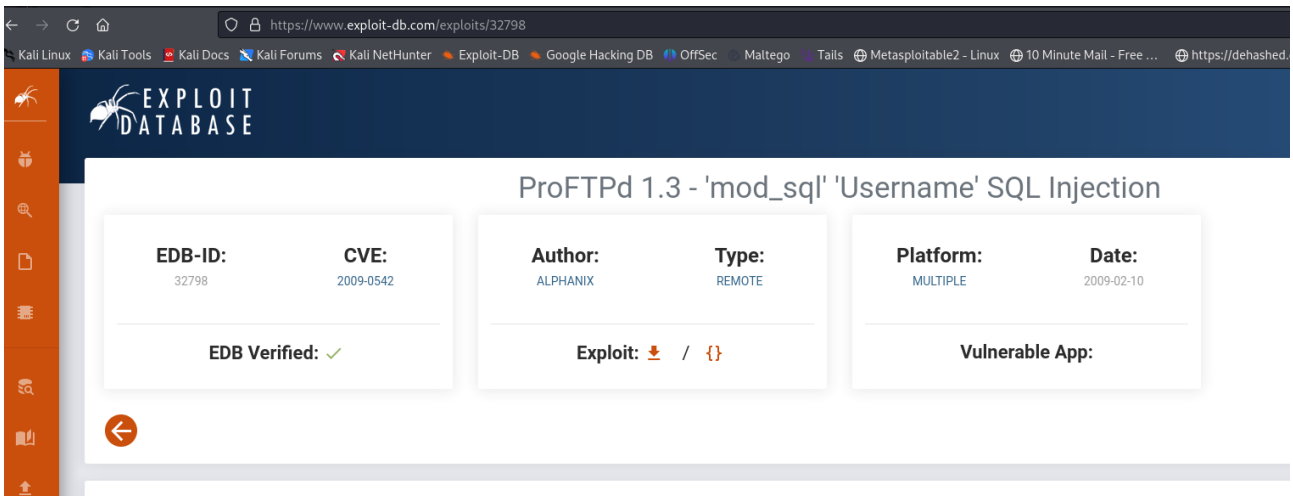
Escaneando con dirb obtenemos:

Este servicio tiene una versión de la cual se descubrio un exploit público de 2008 y se aconseja actualizar la versión.

Vemos el servicio ProFTPD 1.3.1

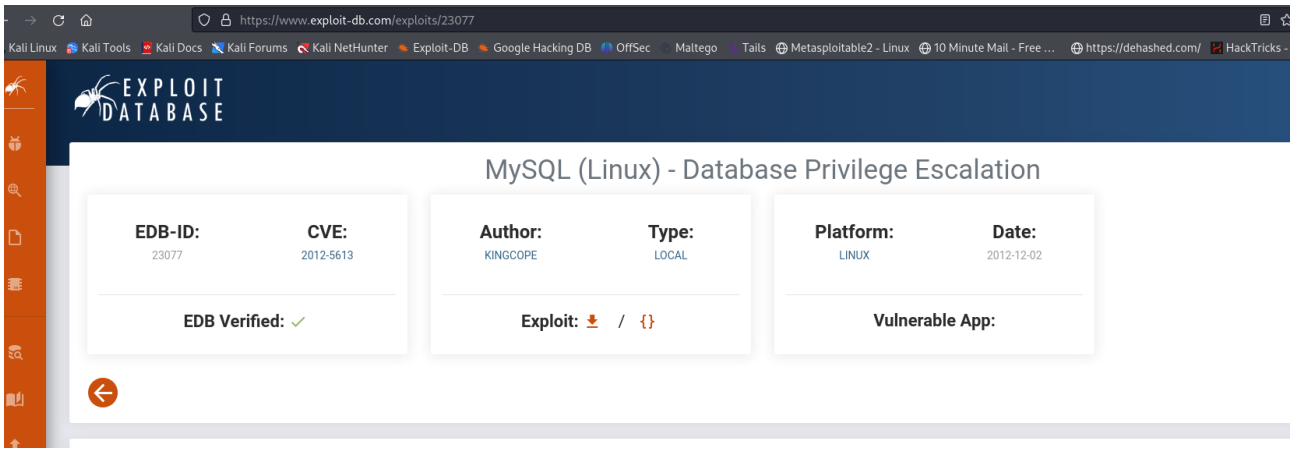


Buscamos en google y encontramos:



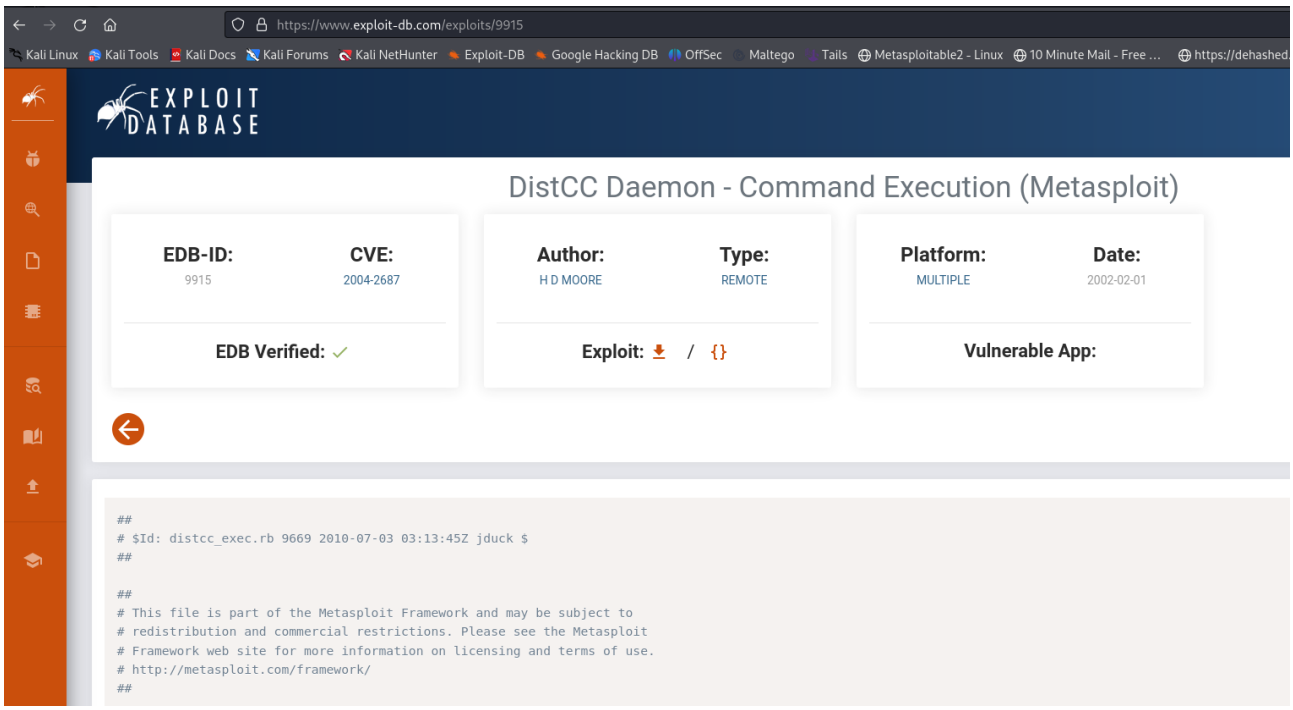
pasa lo mismo que el anterior, tiene una vulnerabilidad descubierta en 2009, se aconseja al cliente actualizar el servicio.

El servicio MySQL 5.0.51a-3ubuntu5, buscamos y nos da esta vulnerabilidad, que es una escalada de privilegios del año 2012:

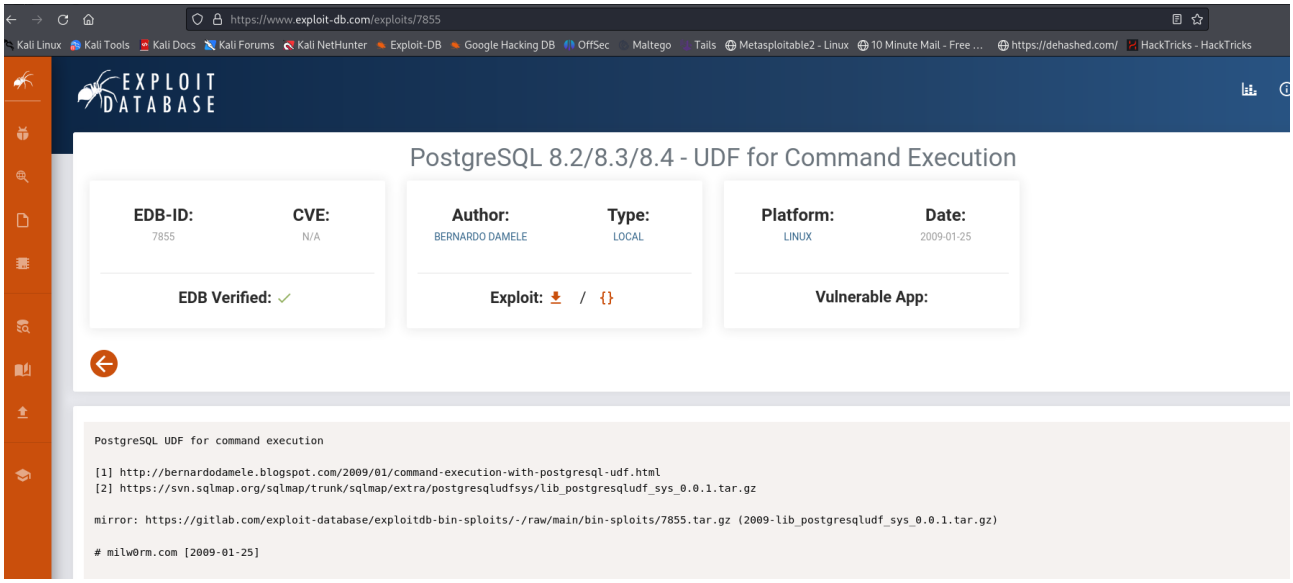


Se aconseja actualizar el servicio.

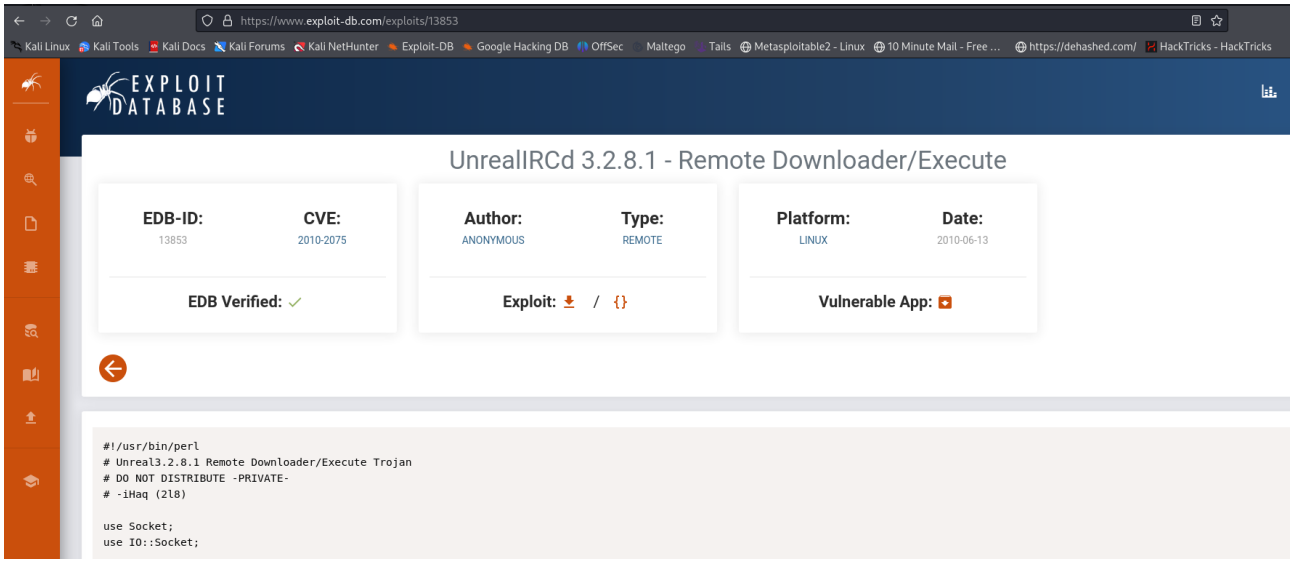
El servicio distccd v1 al buscar nos da esta vulnerabilidad, ejecución de comando:



El servicio PostgreSQL DB 8.3.0, encontramos la siguiente vulnerabilidad ejecución de comando:

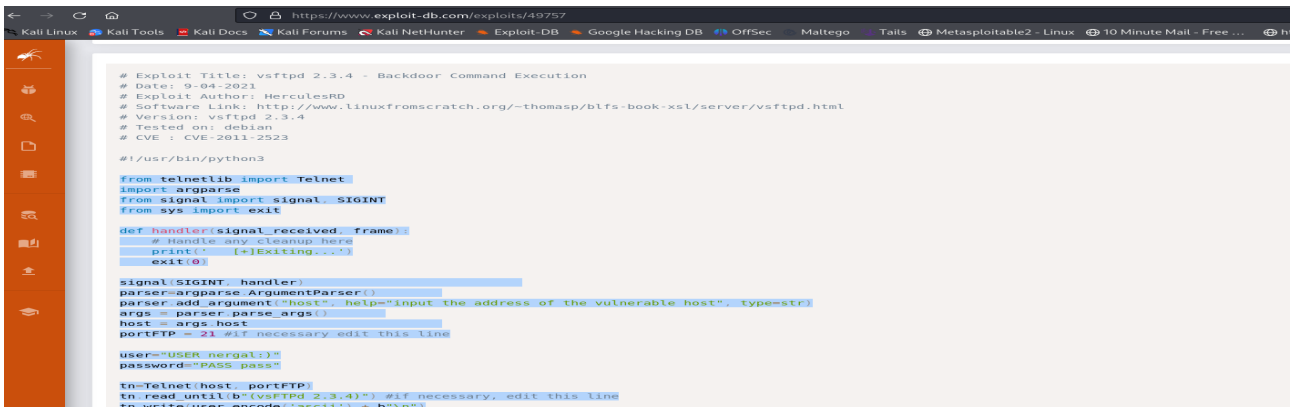


El servicio UnrealIRCd 3.2.8.1, tiene el siguiente exploit:

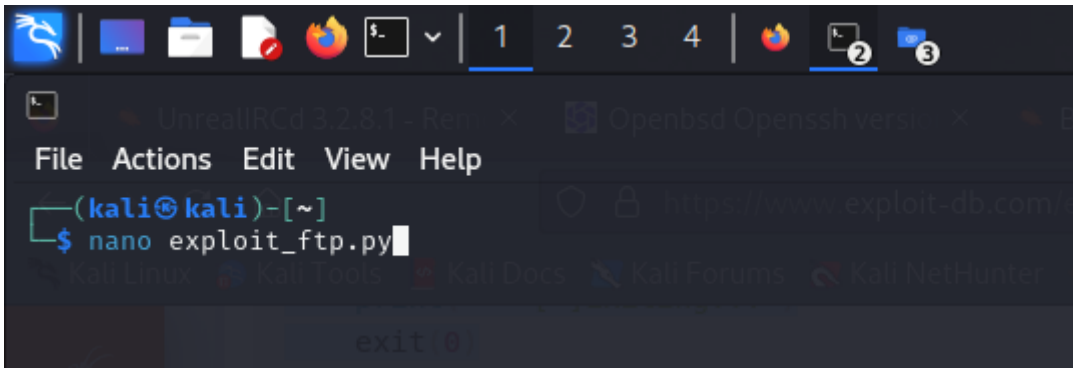


3 EXPLOTACIÓN MANUAL

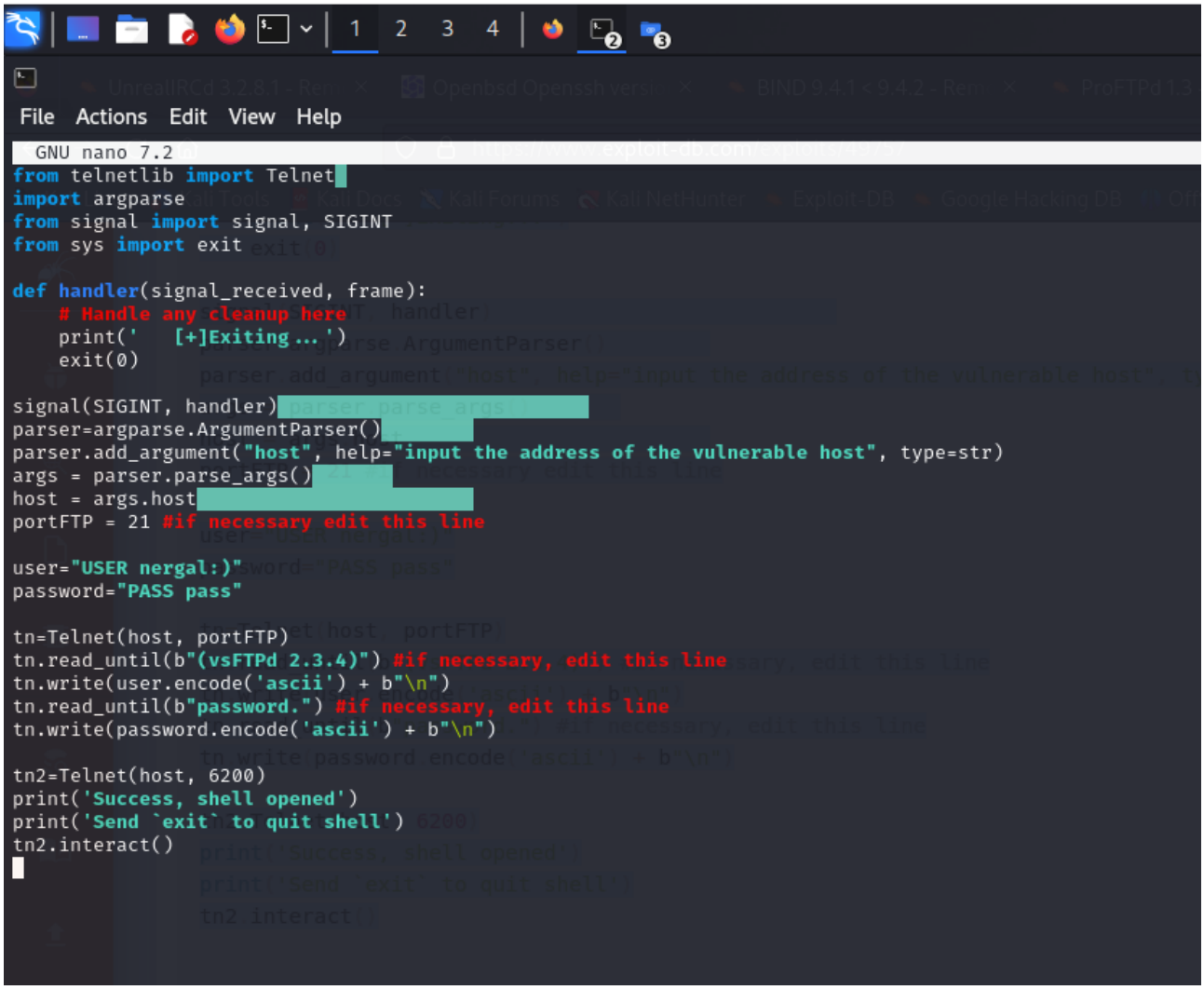
En el exploit vsftpd `2.3.4` tenemos un código python, lo copiamos:



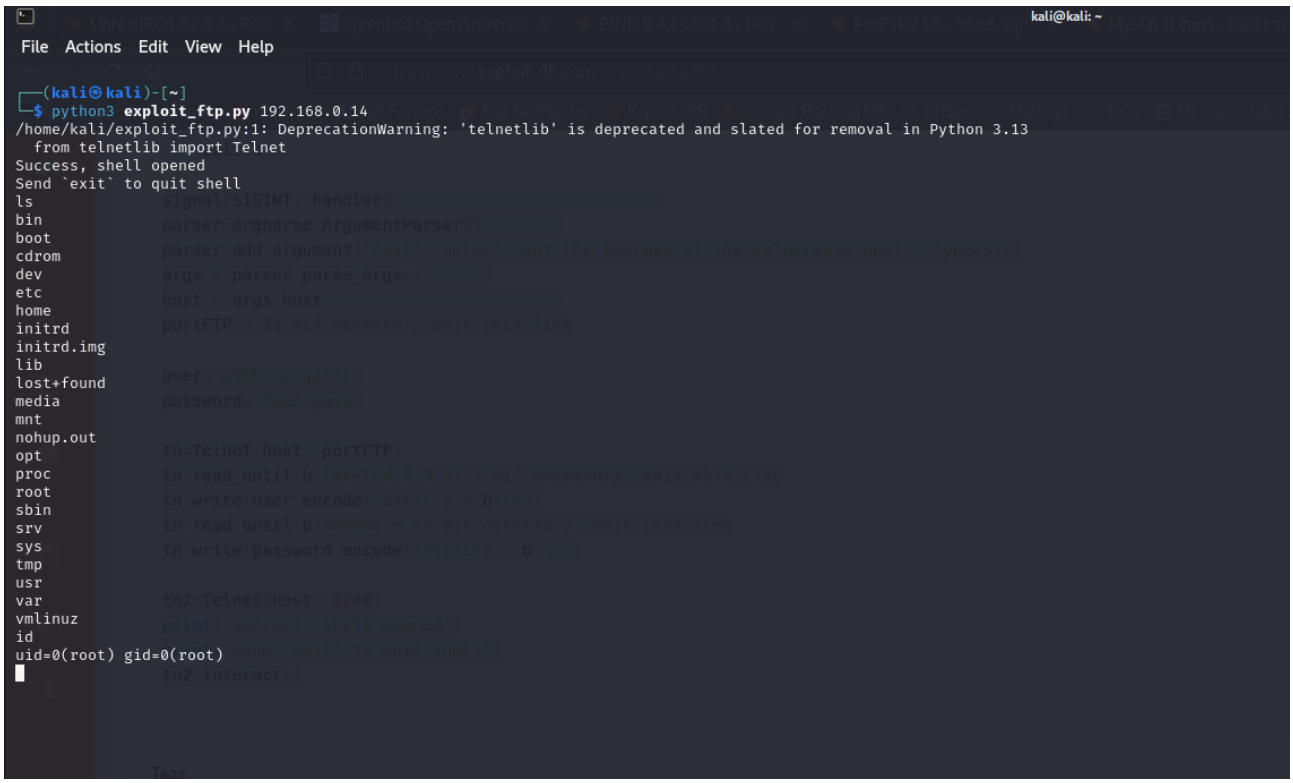
vamos a línea de comandos y abrimos nano:



pegamos el código python:



Lo ejecutamos con python:



entramos en la máquina como usuario root (todos los privilegios).
Esto es una vulnerabilidad CRÍTICA porque tenemos usuario root.
La url del exploit es:
https://www.exploit-db.com/exploits/49757

4 EXPLOTACIÓN AUTOMÁTICA

escribimos en la consola para ejecutar Metasploit:
msfconsole

y entramos en la máquina

3 RESUMEN

Se han encontrado numerosos fallos de seguridad o vulnerabilidades de varios tipos como: inyección SQL, inyección de XSS (código javascript), fallos de software obsoleto o desactualizado sin posibilidad de soporte, fallos de configuración de permisos, así como de autenticación e identificación.

4 POSIBLES SOLUCIONES A LA FALTA DE SEGURIDAD

Se recomienda introducir framework como Spring Security Spring Security (lenguaje Java) para aumentar la seguridad en la autenticación e identificación de usuarios de la aplicación, ORM ´s como Hibernate Hibernate. Everything data o MyBatis MyBatis (github.com) para el control de las consultas SQL.

También se recomienda revisar la configuración de la aplicación y su actualización.