SNP REPORT

Linux vulnerability

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

###### CVE: [2015-1328](https://nvd.nist.gov/vuln/detail/CVE-2015-1328).

Shuhaib A.R.A

IT19366128

Contents

1. Introduction
2. How the vulnerability was found
3. When the vulnerability was found
4. What is the damage it could cause?
5. The exploitation techniques
6. What is the exploitation method is chosen
7. Screenshots of the exploit
8. Conclusion
9. References
10. **Introduction**

This is an privilege escalation attack which is done on Ubuntu with a version of 14.04, It can be done on 12.04, 14.10 and 15.04 also, according to the website (exploit-db) it is done as local attack on but we will be doing it as a remote attack using kali Linux 3.19 version to download and send the file to the Ubuntu d=server in order to escalate privileges. This attack is done using an exploit code written in c language. The main target of this code is to attack the kernel in it. In Ubuntu it does not check permissions for file creation in the upper files system directory, which allows us to obtain root access by leveraging a configuration in which overlays is permitted in an arbitory mount space.

1. **How the vulnerability was found**

The Vulnerability was mainly found on exploit-db website where it has the exploit code and method of doing it as local attack but many other websites were also used in order to make it as a remote attack.

1. **When the vulnerability was found**

This exploit code was found in the mid of 2015 to be specific was on the 15th of June 2015, by the author called Rebel and by the support of Kaliman,Beist. The vulnerability was identified on the 24th of May 2015 which just took correctly 22 days to exploit it.

1. **What is the damage it could cause?**

The damage it could do to the Ubuntu server will be dangerous, because it lead to a privilege escalation attack in order to gain root access to the server. By doing so sensible files and other important information could be taken without root access

1. **The exploitation techniques**

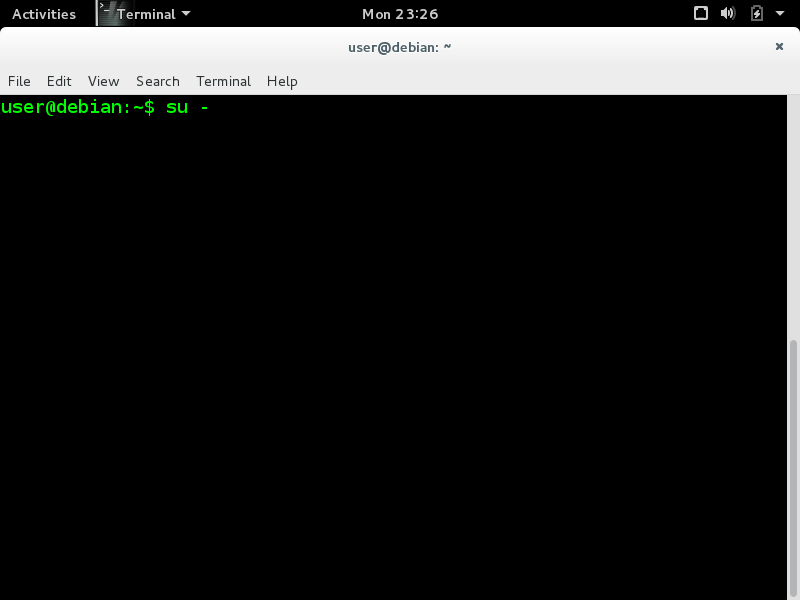
There two exploitation techniques one by doing it on the same Ubuntu server which will be a local attack, which is where we download the exploit code and run it in the Ubuntu sever by first typing the command *uname –a.* The other method is by sending the exploit code by the linux kernel,the command used to send the exploit file will be *scp codename.c ubuntu@ipaddress:/home/Ubuntu.* After the file is transferred we should just run the code in the Ubuntu server and gain privileges and this would be a remote attack.

1. **What is the exploitation method is chosen**

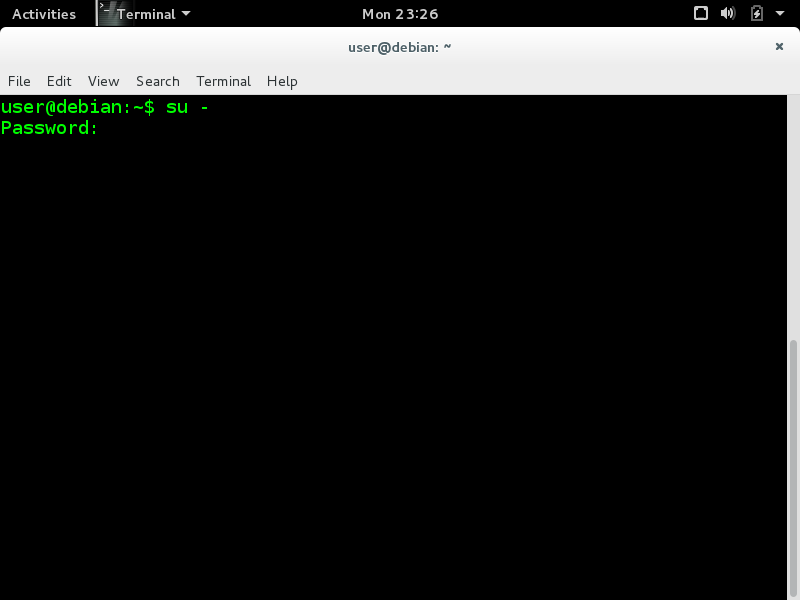
Here the exploitation method chosen would be the remote exploitation method. Because it is more efficient to send a file through the same network than making a specific download for the system by same server.

1. **Screenshots of the exploit**

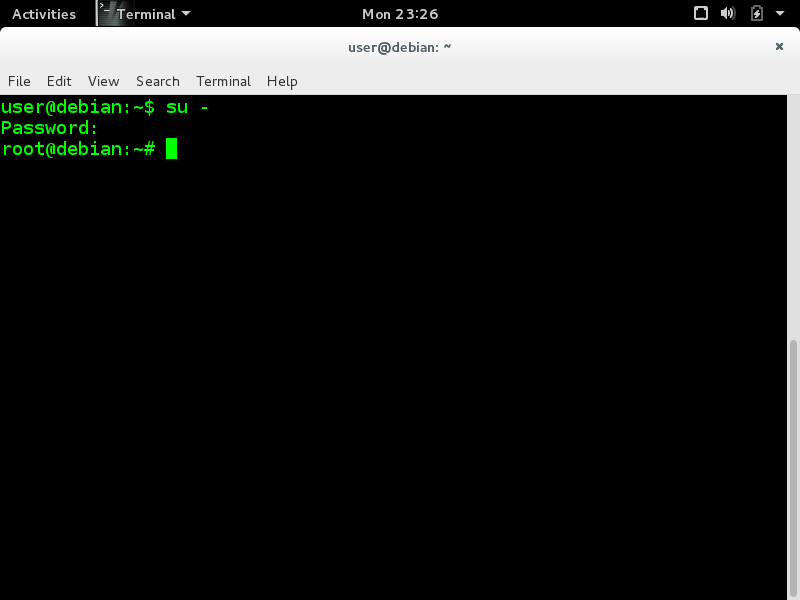
**1st step:** gain root access in the Linux kernel by using root user *by “su -”* command*.*

****

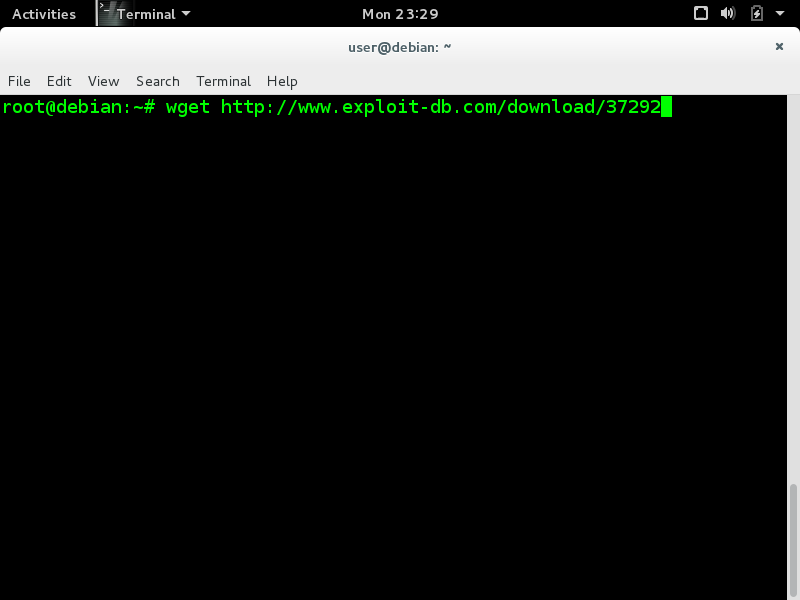
**2nd step:** enter the password



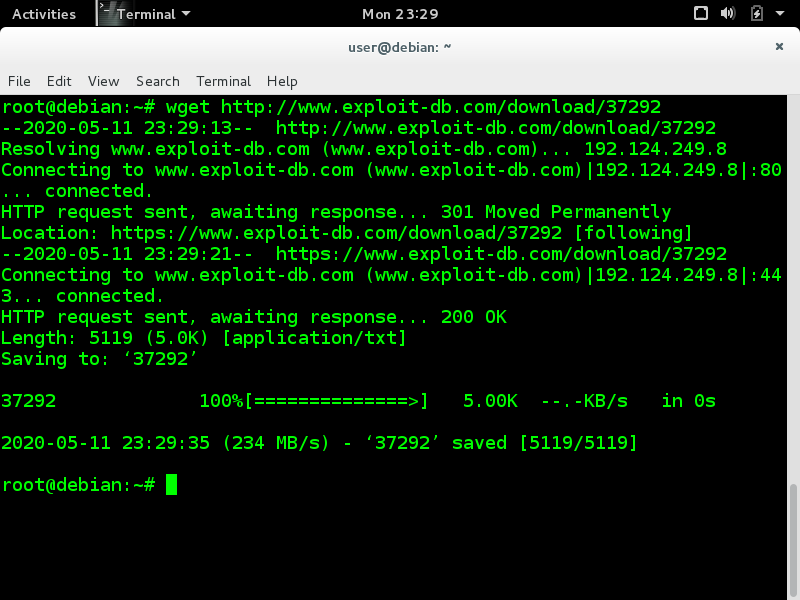
**3rd step:** gain root privileges as we can see the “$” sign is changed to “#” sign



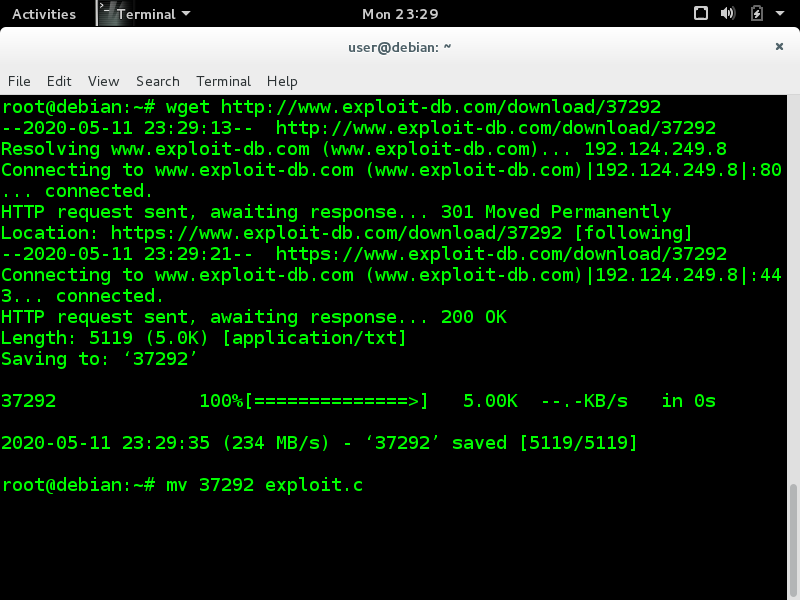
**4th step:** download the exploit code from the exploit database site byusingthe *“wget”* command*.*



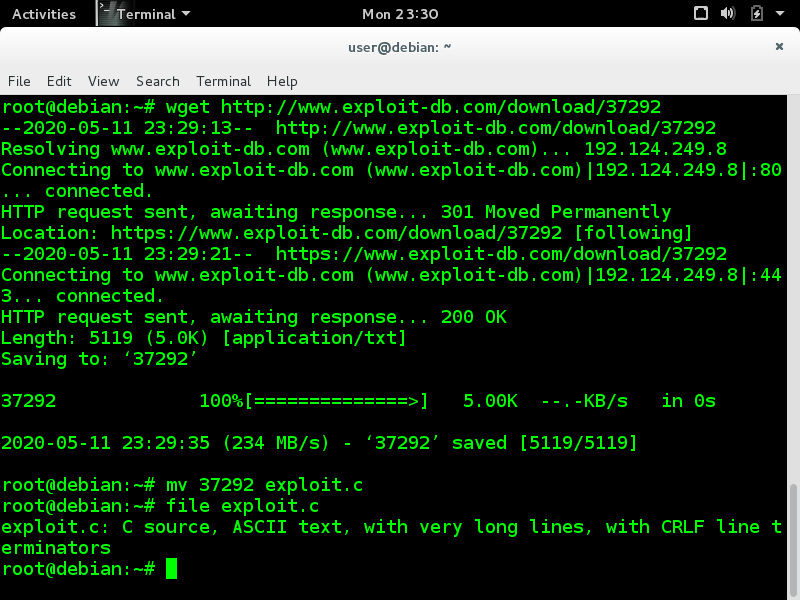
**5th step:** check the name of the exploit file (in this case it is “37292”).



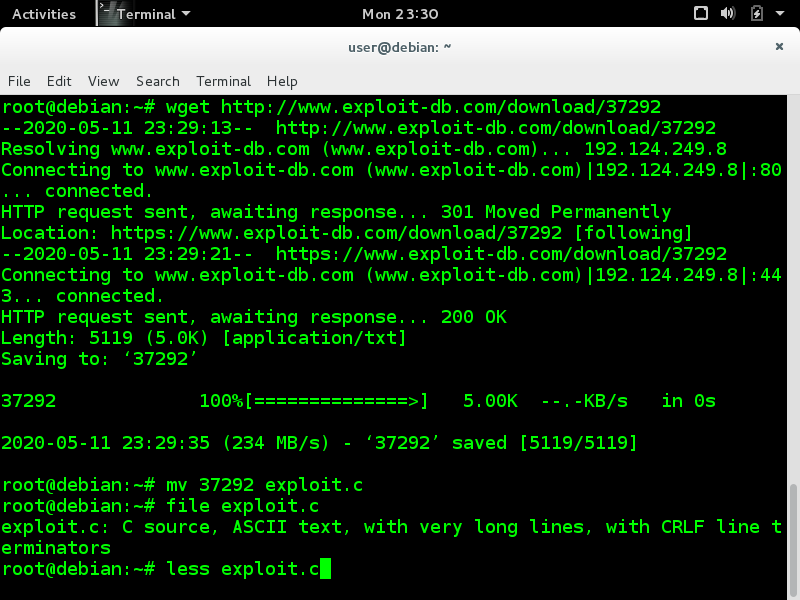
**6th step:** change the name of the exploit file with an extension of “.c” by *“mv”* code*.*

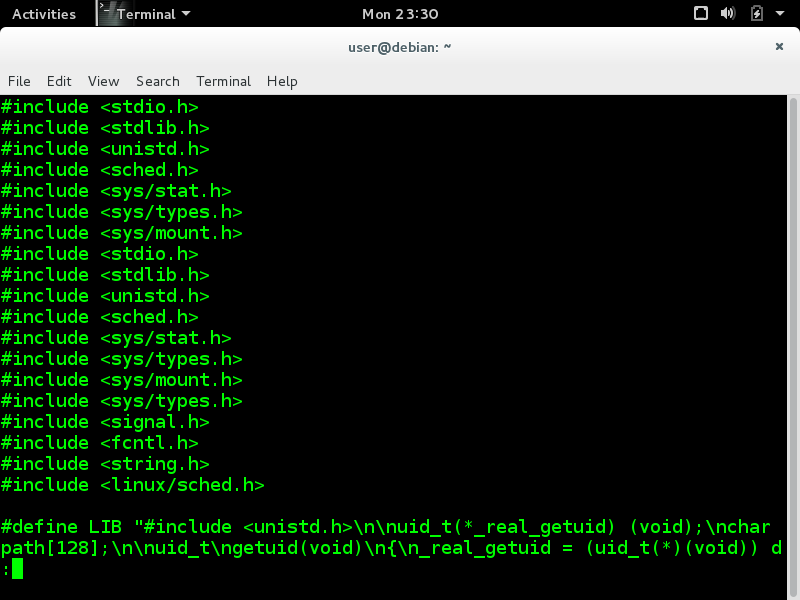


**7th step:** check whether the file is a “c” file by using the *“file nameofthefile.c”*.

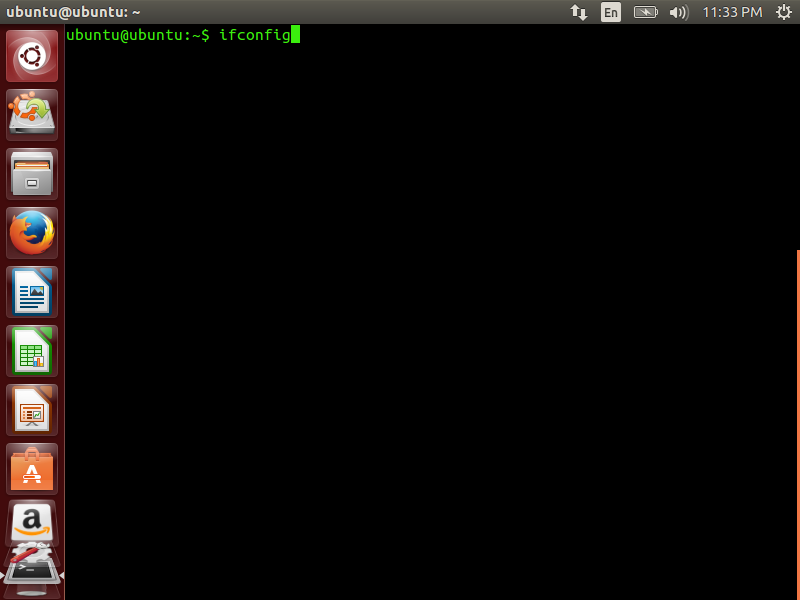
****

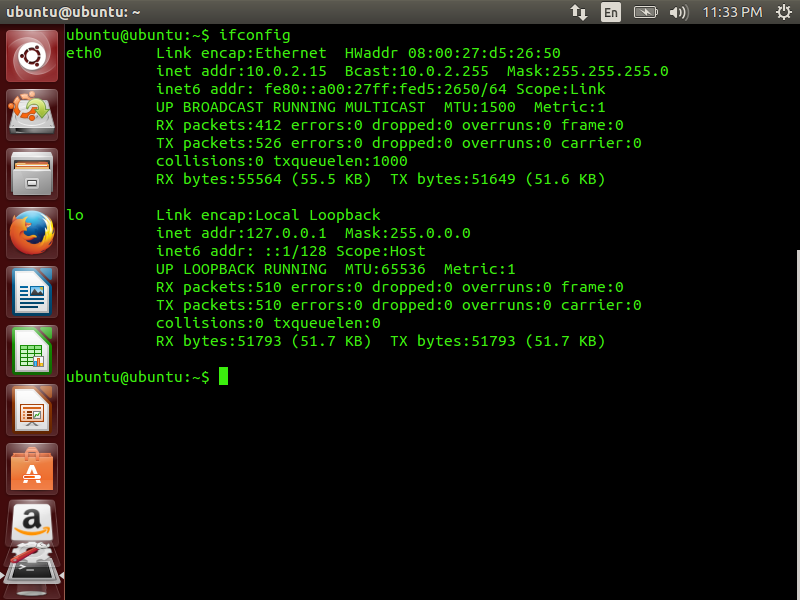
**8th step:** checking whether the code is correct by typing *“less nameofthefile.c”.*



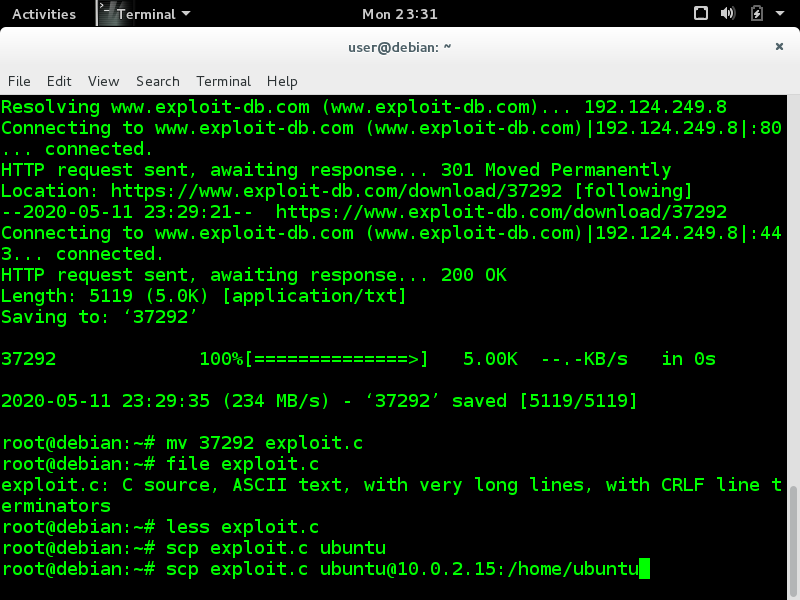


**9th step:** get the Ubuntu machines ip address bu typing *“ifconfig”.*

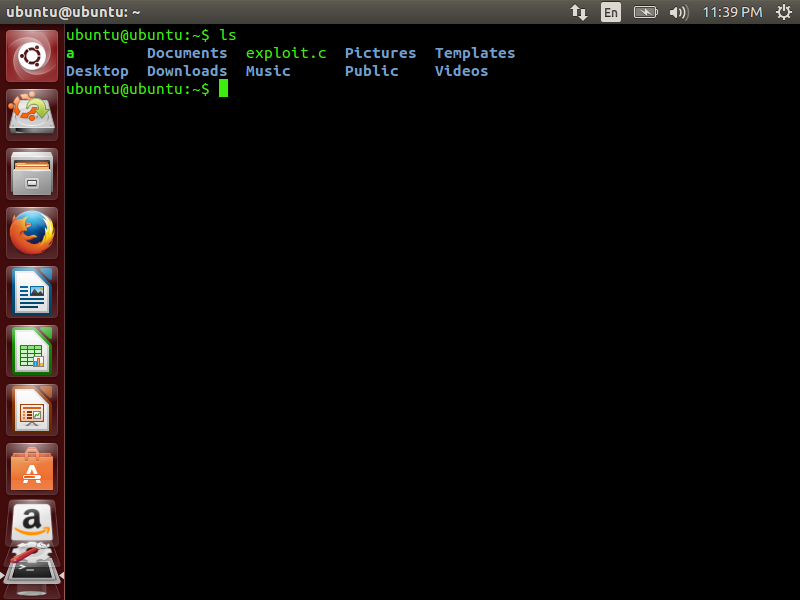




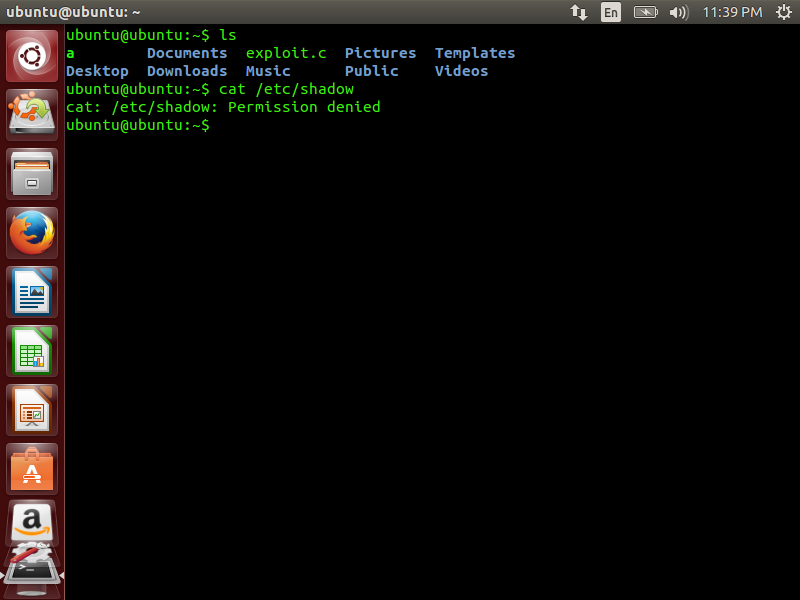
**10th step:** send the code to the host machine by the *“scp nameofthefile.c ubuntu@ipaddress:/home/Ubuntu”* code.



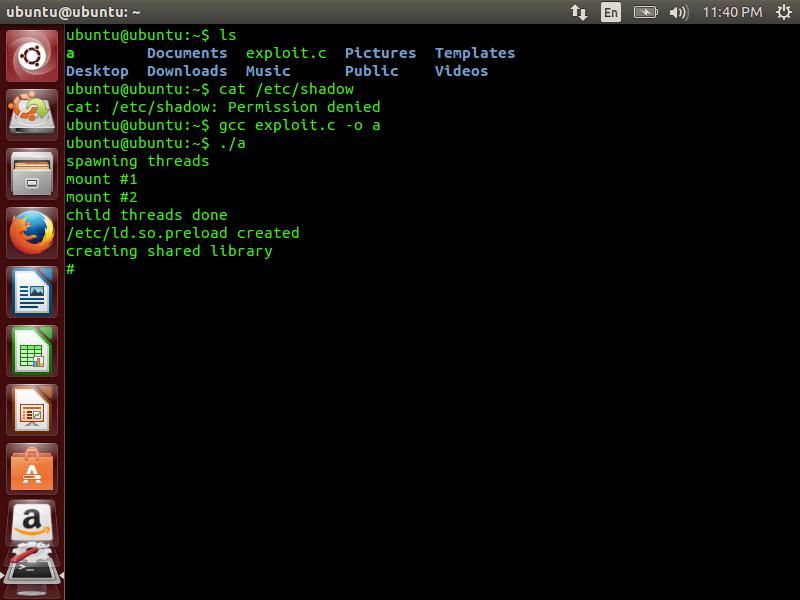
**11th step:** run the *“ls”* command in Ubuntu.



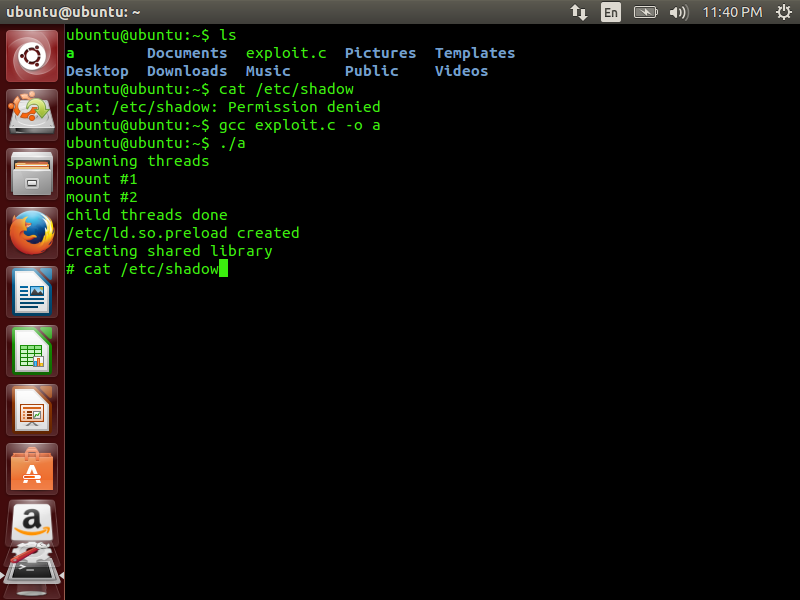
**12th step:** trying to check is there root privileges in the account by the command *“cat /etc/shadow”.*

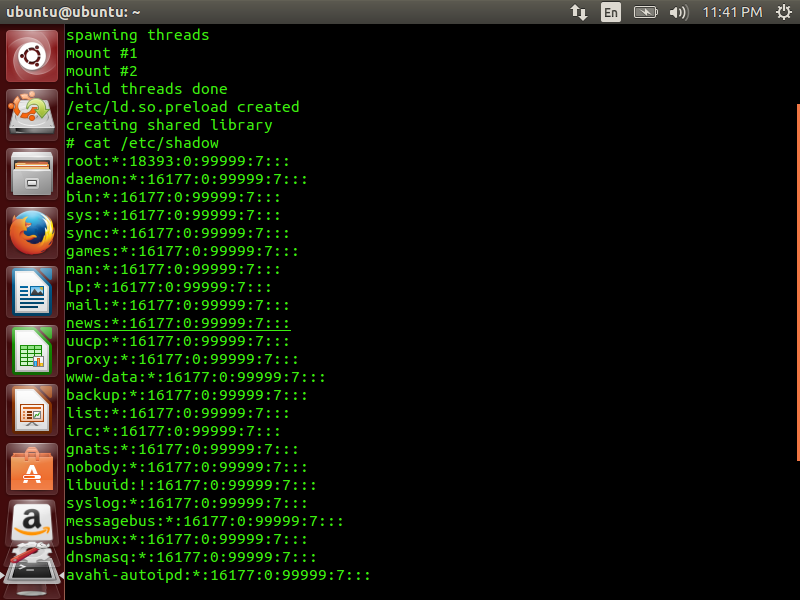


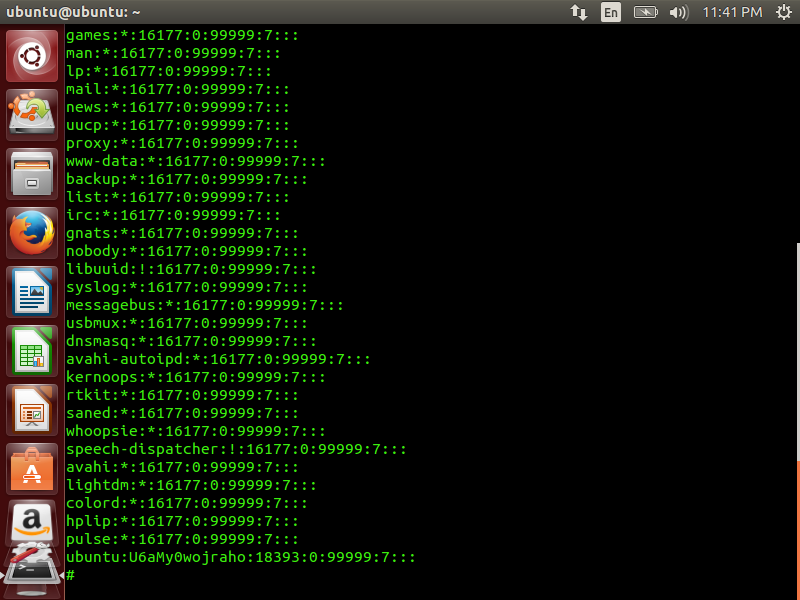
**13th step:** now we should compile the file in by using *“gcc nameofthefile.c –o newname ”*  and run the file with the *“./newname”* command.



**14th step:** trying to check is there root privileges in the account by the command *“cat /etc/shadow”* after executing the file.







1. **Conclusion**

Finally we could find enough vulnerabilities in any operating systems in order to make unauthorized activities possible, for example privilege escalation, DDos attacks etc. This should be prevented and patched on time in order to stay safe from cyber-attacks. This attack which I explained has base score of 7.8 which is a very important vulnerability, so if we could prevent the error which is where the version does not check permissions for file creation in the upper files system directory, we could prevent attacks which try to leverage their privileges in order to gain root access.

1. **References**

**1. References used to understand the “C” code:**

[www.techonthenet.com](http://www.techonthenet.com)

[www.geeksforgeeks.com](http://www.geeksforgeeks.com)

[www.qnx.com](http://www.qnx.com)

man7.org

[www.includehelp.com](http://www.includehelp.com)

[www.stackoverflow.com](http://www.stackoverflow.com)

[www.cplusplus.com](http://www.cplusplus.com)

[www.linuxhint.com](http://www.linuxhint.com)

**2. References used to understand the attack**

[www.exploit-db.com](http://www.exploit-db.com)

nvdnist.gov

cve.mitre.org

urlmon.com

[www.tenable.com](http://www.tenable.com)

[www.wikihow.com](http://www.wikihow.com)

[www.tecadmin.net](http://www.tecadmin.net)

[www.tecmint.com](http://www.tecmint.com)

**3. References used to make the local attack an remote attack**

[www.serverfault.com](http://www.serverfault.com)

[www.linode.com](http://www.linode.com)

linuxconfig.com

[www.carnaghan.com](http://www.carnaghan.com)

[www.vultr.com](http://www.vultr.com)

process.st

[www.bencane.com](http://www.bencane.com)

[www.digitalocean.com](http://www.digitalocean.com)

[www.youtube.com](http://www.youtube.com)