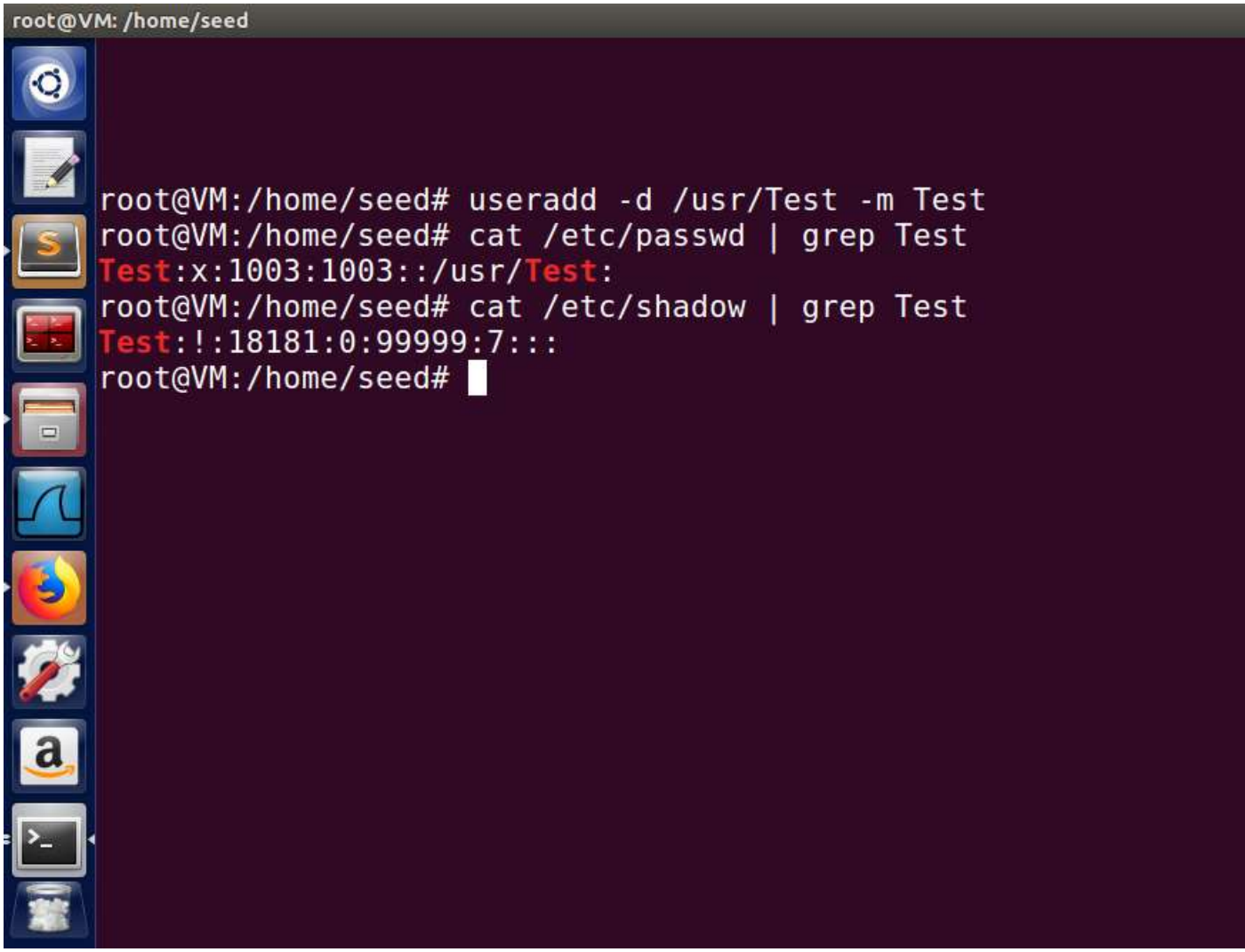
Assignment 06

RISHI KUMAR SONI 1001774020

## Task 1: Choosing Our Target

Observation

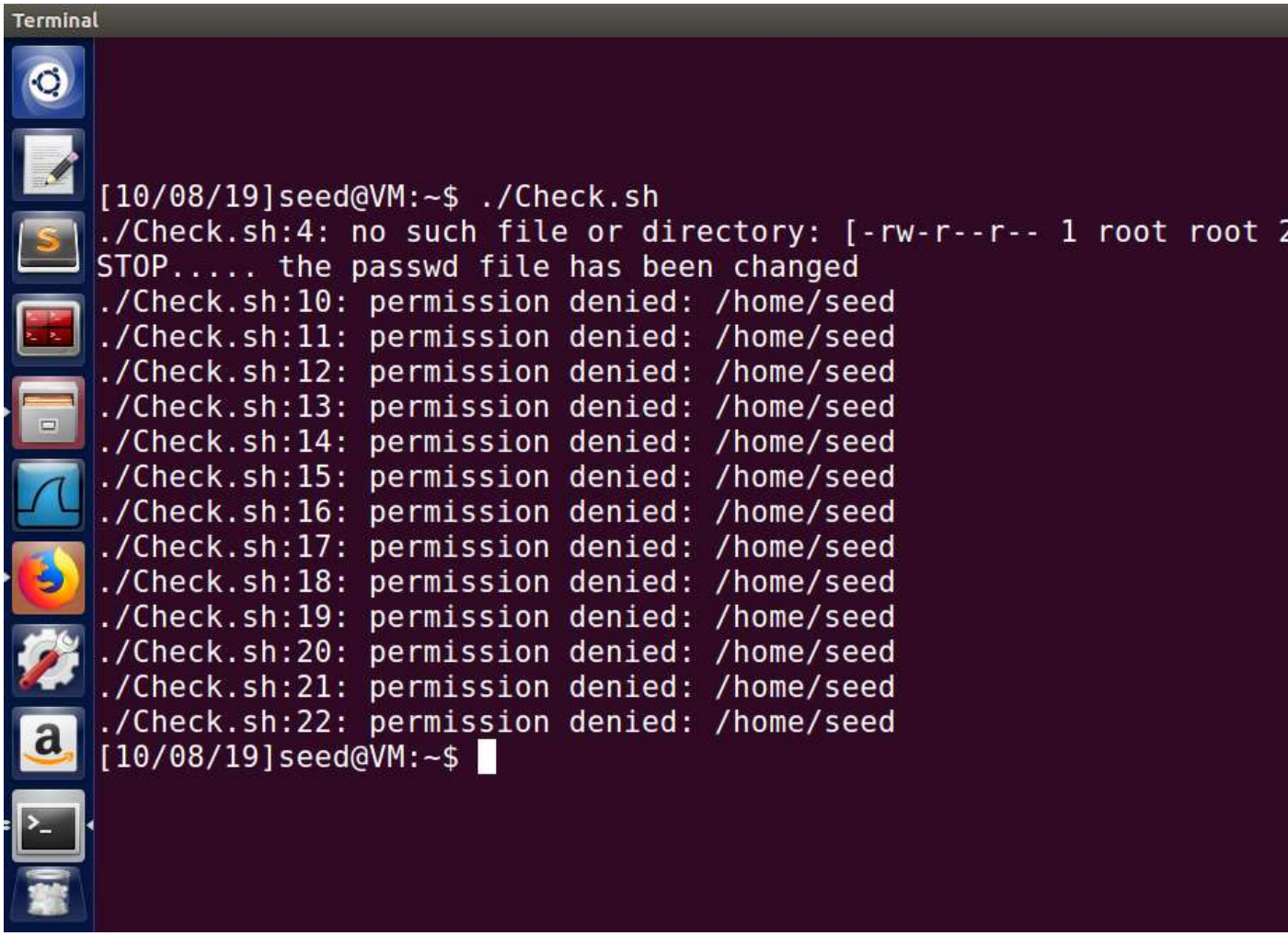


**Explanation:**

The third column in the file `/etc/passwd` denotes the UID of the user. Because `Test` account is a regular user account. If we change this entry to 0, `Test` will becomes `root`.

## Task 2: Launching the Race Condition Attack

| Observation |
| --- |



**Explanation:**

For this task, we disable the sticky protection mechanism. We have to show the Race Condition , it can be done by adding new line in the passwd file.Repeat.sh is the shell code that takes the value from the input.txt and give it input vulnerable program vulp.c.

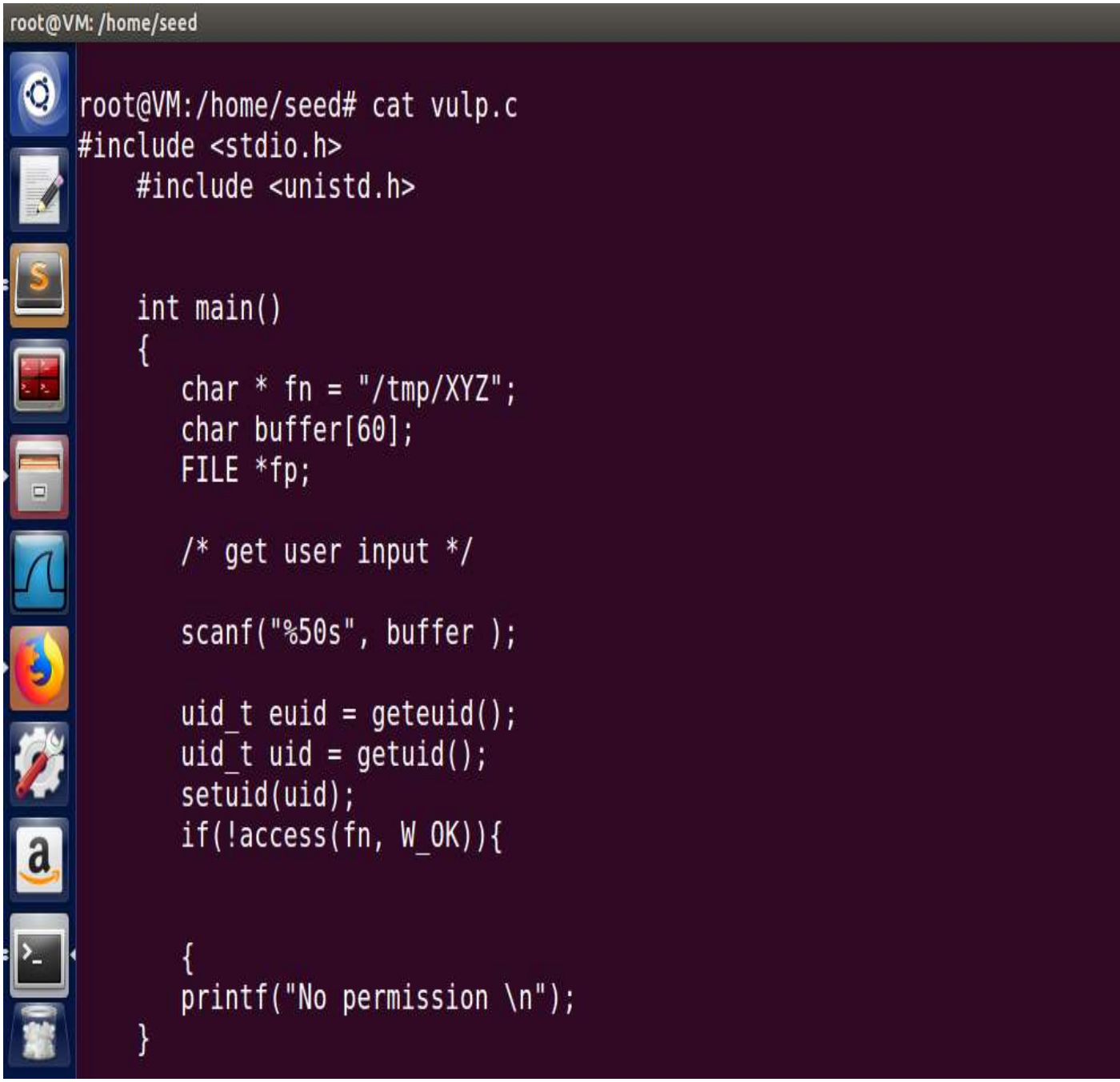
*We can see after multiple attempts at exploiting the race condition, out attack runs and the message is displayed.*

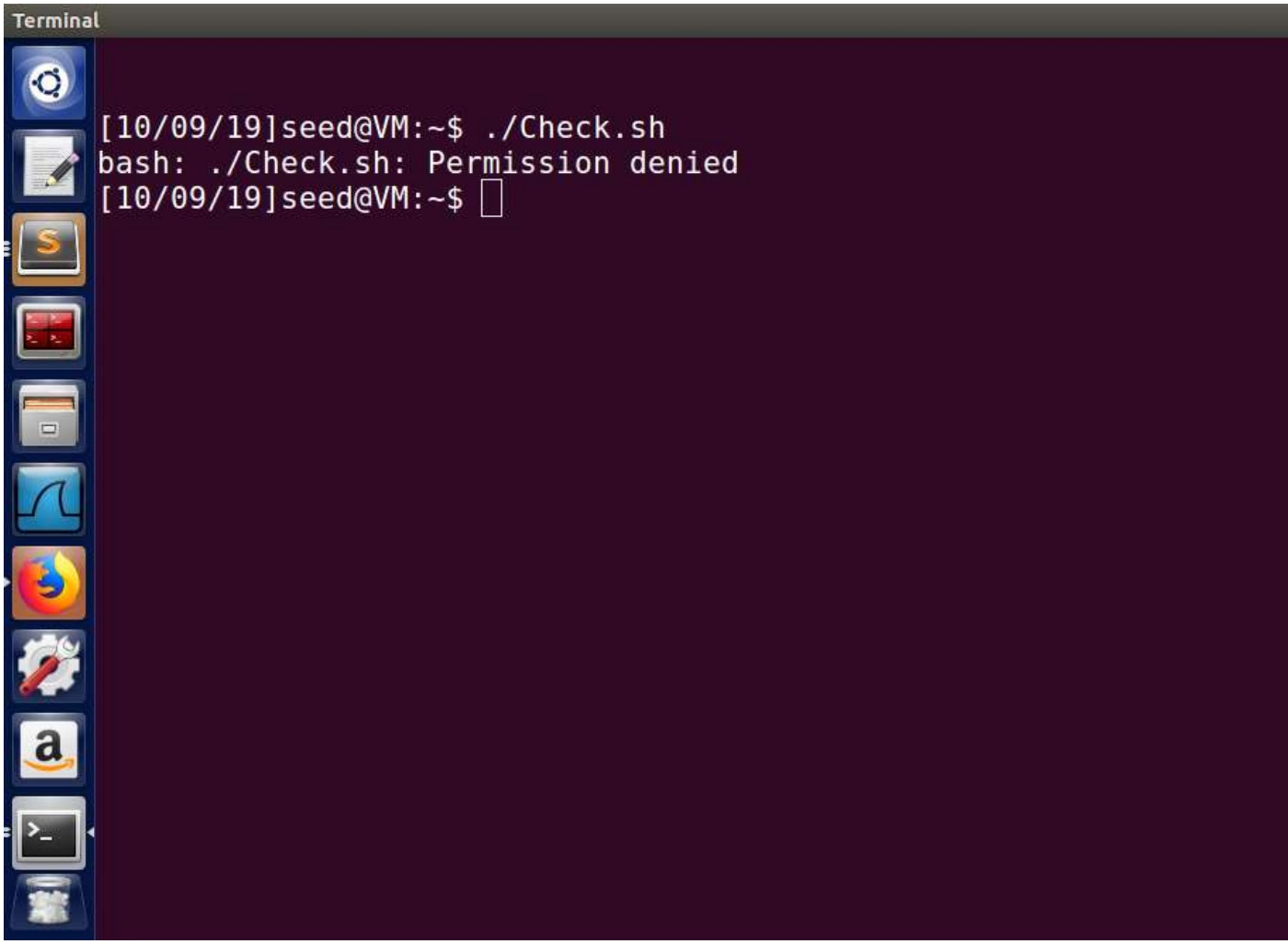
Output

We can see after the race condition , out attack runs and message is displayed by check.sh.

**Task 3: Countermeasure: Applying the Principle of Least Privilege**

Observation


root@VM: /home/seed
root@VM:/home/seed# cat vulp.c
#include <stdio.h>
#include <unistd.h>
int main()
{
char * fn = "/tmp/XYZ";
char buffer[60];
FILE *fp;
/* get user input */
scanf("%50s", buffer );
uid_t euid = geteuid();
uid_t uid = getuid();
setuid(uid);
if(!access(fn, W_OK)){
{
printf("No permission \n");
}

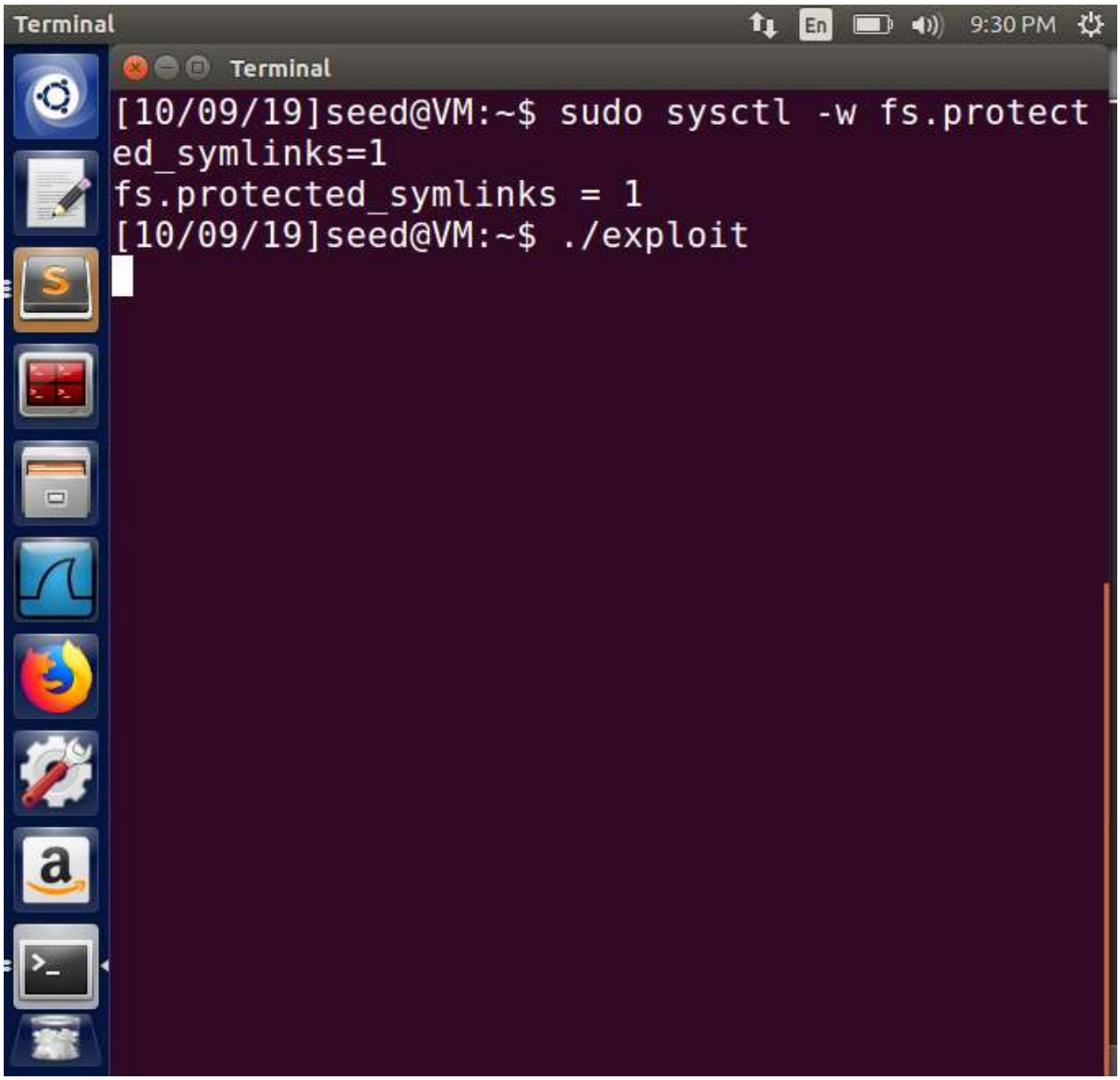



**Explanation:**

We modified the vulnerable program so that we downgrade the privileges before the checks and then revise the privileges at the end of the program. But after perform the task again, it doesn't work.

**Task 4: Countermeasure: Using Ubuntu's Built-in Scheme**

| Observation |
| --- |
| |




## Explanation:

In this , we turn on the sticky bit protection and perform the same the attack.Our attack is failed.

1. How does this protection scheme work?

A **Sticky bit** is a permission **bit** that is set on a file or a directory that lets only the owner/root of the file/directory or the root user to delete or rename the file.

2. What are the limitations of this scheme?

Limitations:

- Works only for the directories where sticky bit in on or working.
- It works in some of the cases only. Race condition would work in the directory or file which is owned by the root and which can be modified.