Man Tik Li

CS 377 - 001

November 30, 2020

**Lab 5**

## Initial Setup

**This lab will complete on Ubuntu version 12.04.**

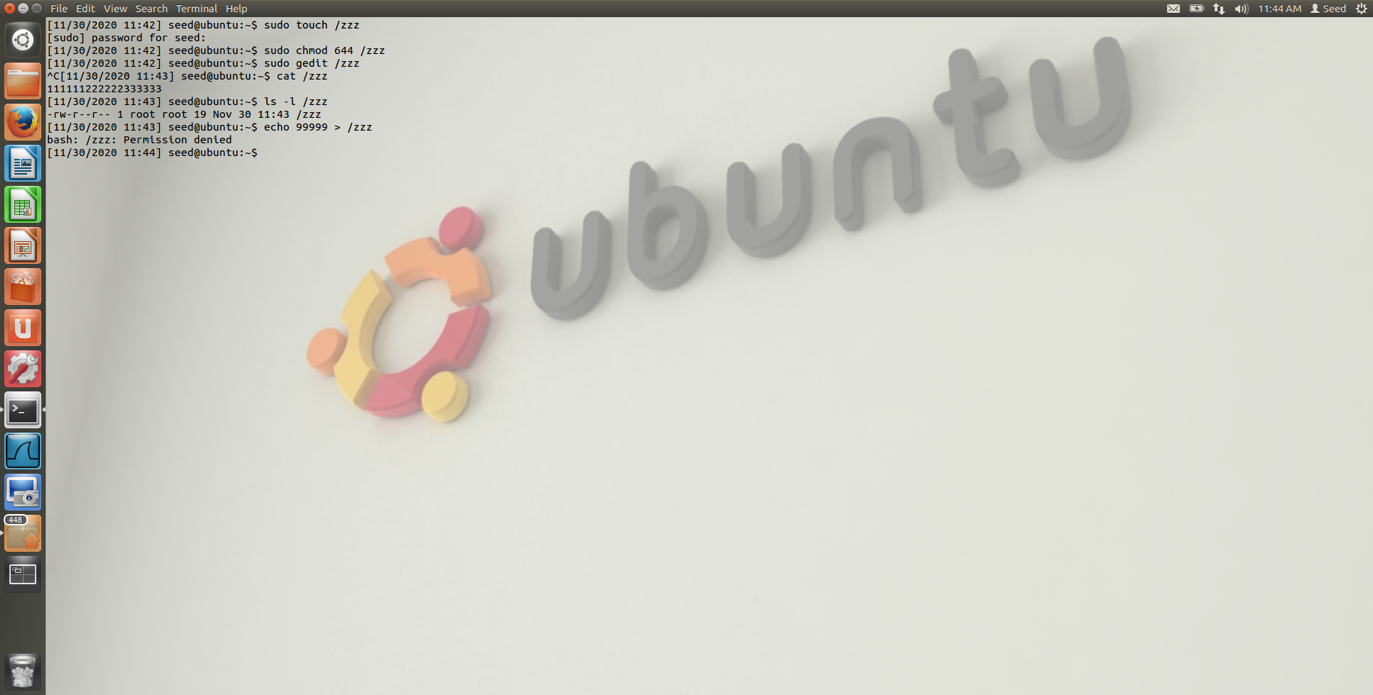
Graphical user interface

Description automatically generated

## Task 1

2.1 – Create a dummy file and modify /zzz

We modify the file /zzz to exploiting the dirty cow.

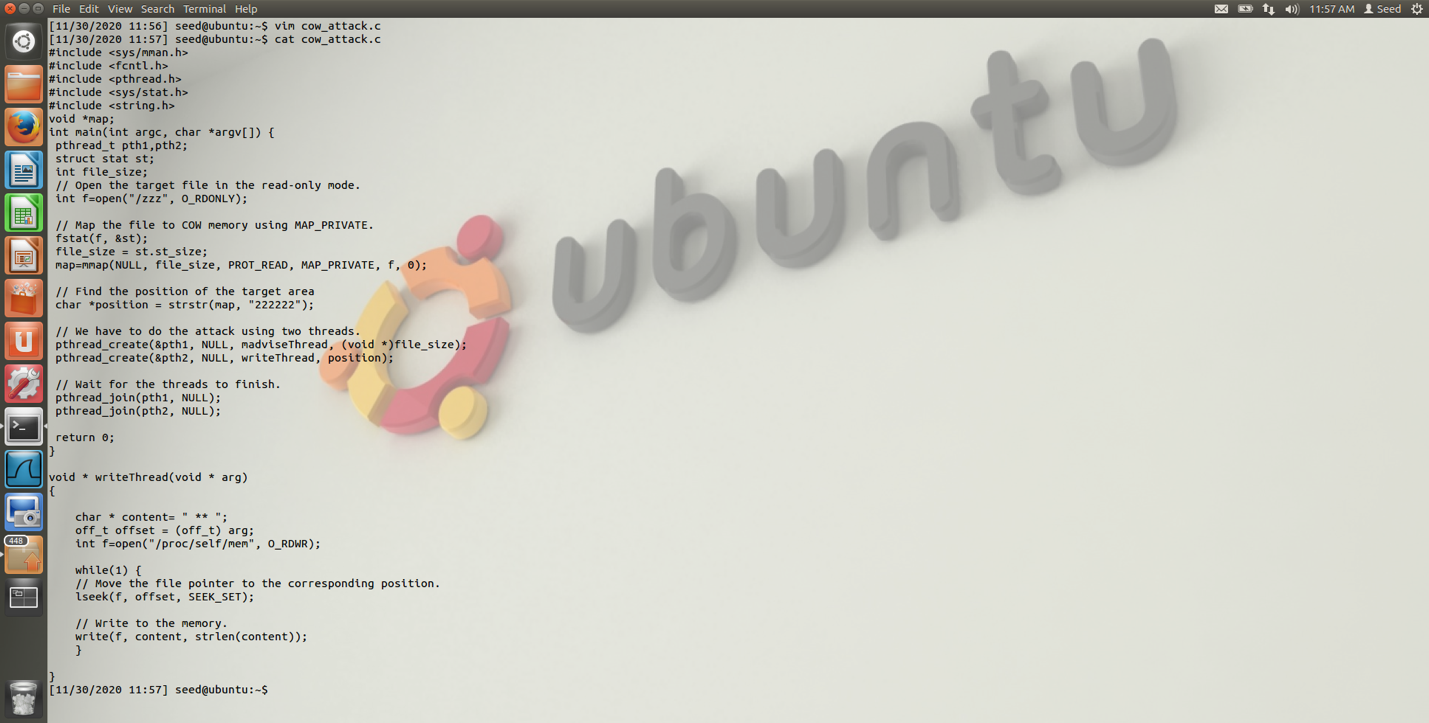


2.2 – Set Up the Memory Mapping Thread

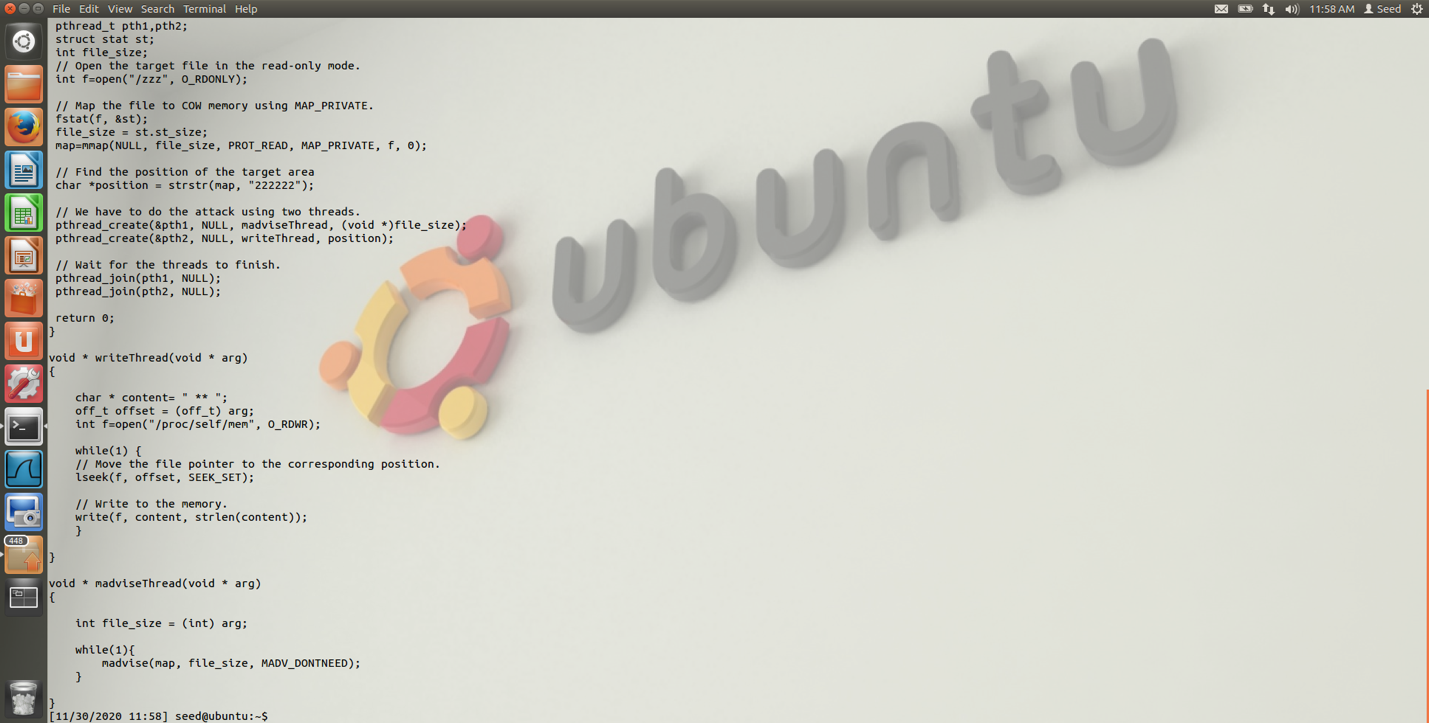
Text

Description automatically generated

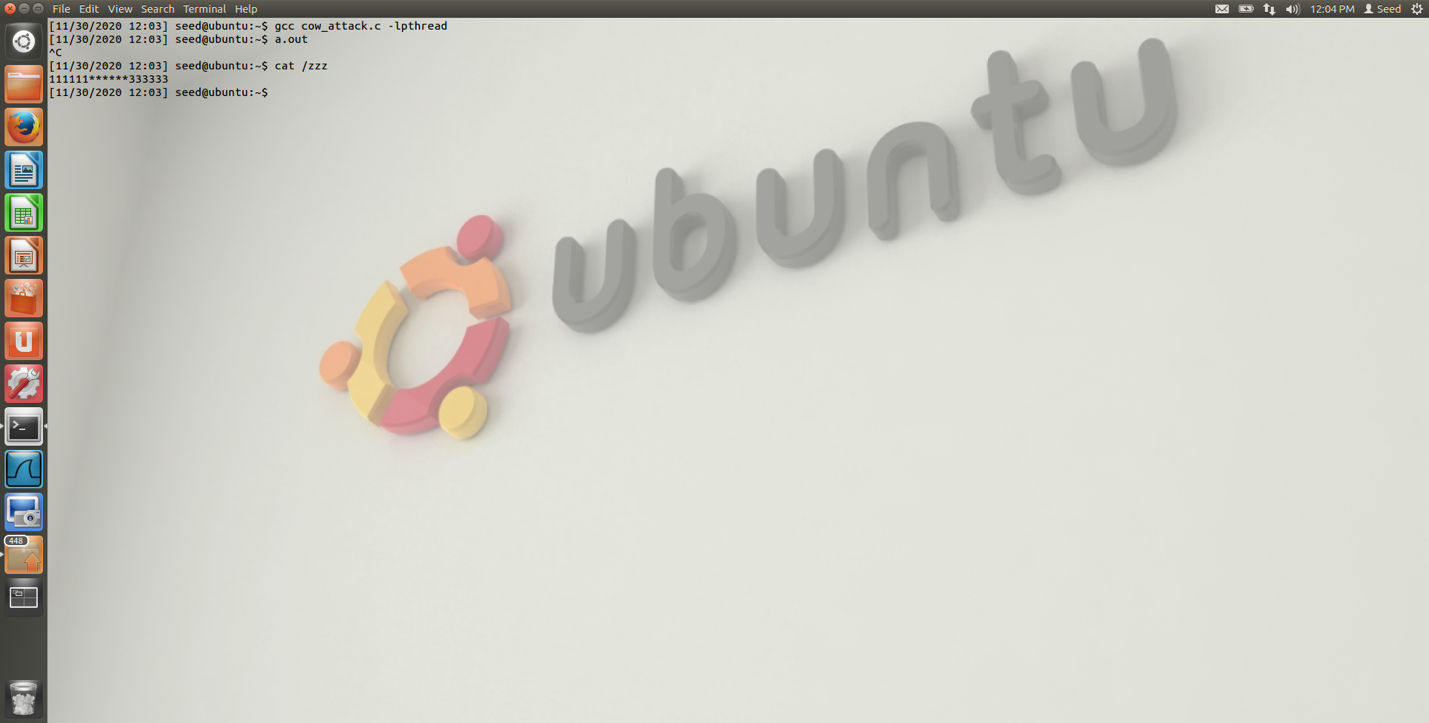
2.3 – Adding writeThread() method into cow\_attack.c



2.4 – Adding madviseThread() into cow\_attack.c



2.5 – Launch the attack

The attack is success after I ran the a.out for coupon seconds. The 2 had replaced with \*.

## Task 2

I changed the open directory to “/etc/passwd”, position with “charlie:x:1001:1002”, and content to “Charlie:x:0000:1002”

Text

Description automatically generated

I use attack.c program to launch the attack on /etc/passwd and successful in giving root privileges to Charlie.

