Lab 4: Dirty COW Attack Lab

Samuel Shen Prof. Kadri Brogi

CUNY John Jay College of Criminal Justice

November 6, 2019

1. Introduction

Today, we will investigate and experience with the Dirty COW vulnerability. Dirty COW vulnerability is similar to the race condition vulnerability and existed in the Linux kernel since the September 2007. This vulnerability was discovered and exploited in October 2016.

In order, for us to experiment with this vulnerability, we will be using the following:

* SeedLab Ubuntu 12.04 VM
* The Provided vulnerable file: cow\_attack.c

1. Task 1: Modify a Dummy Read-Only File

In this task, we run a test dirty COW attack on a dummy read-only file. We will create “/zzz”, add “111111222222333333” and attempt to change “222222” to “\*\*\*\*\*\*”. The first thing we will do is create the file it, add the text, change to read-only, and attempt to edit it to ensure the file is read-only:

A screen shot of a computer

Description automatically generated

Once we have our file as read-only, we will now launch “cow\_attack.c” to change the text “222222” to “\*\*\*\*\*\*”:

A picture containing indoor, wall

Description automatically generated

1. Task 2: Modify the password File to Gain the Root Privilege

Since we were successful in changing “222222” to “\*\*\*\*\*\*” we will now launch it on something more real. We will create a new user called “Charlie” and attempt to get root access.

A picture containing text

Description automatically generated

Once we have created the user Charlie, we can see that Charlie is just a standard user from “charlie:x:1001:”. We will now launch the attack on “/etc/passwd” to change charlie from standard user to root.

A picture containing indoor

Description automatically generated

As you can see from the screenshot above, we have modified cow\_attack.c to launch to /etc/passwd. Once it ran, we changed user to charlie and can notice that charlie now has root access.