Linux Kernel Module Assignment

CSIS 443

Professor OMalley

James Riley Dorough

Liberty University

November 20th, 2021

**Introduction**

This lab exercises the ability to understand, modify, and implement kernel modules. With this understanding of functionality, stems an understanding of the vulnerability and security requirements of access to modification or insertion of kernel modules and device drivers.

**Lab Work & Implication**

To complete this lab, I have spun up a fresh Ubuntu box. My clone of a Kali box required slightly different headers and commands to complete the lab. Due to this I needed a fresh, compatible environment. After the new box was ready, I began following the listed instructions and researching how to modify the kernel module.

Text

Description automatically generatedI attempted various methods of inserting and modifying the kernel module to allow for reading from a device file. Eventually I found a blog that contained the modifications that I required to take input from the device input (Kutkov, 2021). The modifications made are noted in the image on the next page.

**Text

Description automatically generated**

I believe that most of this code it not required to complete the lab. However, including the additional bounds checking and output debugging phrases assisted in my learning of the functionality of different aspects of the kernel module. After making the kernel object, inserting it, create the character device file, and allowing it to be written to; I ran into another bash error which required additional research and updating the system. Finally, I was able to gain the anticipated outcome. Text

Description automatically generated

This lab shows the importance of abstraction and additional layers of security for core functionality of operating systems. Systems that allow for unprivileged access to altering kernel code are already crippled. Ensuring operating system are designed with security and abstraction from the ground up is critical to minimize access to kernel memory. Even with high levels of security we still see various attacks such as buffer overflows and specter attacks. Continual effort must be made to understand the vulnerabilities and improve countermeasures to distance the highest form of system access from its users.

**References**

Kutkov, O. (2021, February 5). *Simple Linux character device driver*. Oleg Kutkov Personal Blog. Retrieved November 21, 2021, from https://olegkutkov.me/2018/03/14/simple-linux-character-device-driver/