Andrew Parker, Alex Cater

CS 493

Dr. Lawlor

11/21/19

Project Writeup Draft

For our project, we have decided to write a linux kernel module capable of providing root. Initially our project plan was to infect a VM with a rootkit and analyze the effects of the rootkit. However, we changed our project to writing our own rootkit and analyzing its effects. So far, our kernel module and give root access to a user as long as they can write to a device and know the correct password. Currently we are trying to implement a keylogger. The key pressed are logged to the kernel. Since we have already created a device, we hope to somehow use the device to log the keypresses. This project helped us gain a much better understanding of the inner workings of the linux kernel and how devices function in linux.

Functionality

- prints to kernel logs
- creates a device ``/dev/ttyR0``
    - has custom read/write/open/release functions
    - "echo 'CS493' >> /dev/ttyR0" gives root access to user
    - able to read string stored in kernel using a userspace program
        - at the moment only works on first read after loading the module. Trying to read again will return an empty string
    - "echo 'keylogger' >> /dev/ttyR0" turns on the keylogger. At the moment, keys pressed are written to the kernel logs.