Andrew Parker, Alex Cater

CS 493

Dr. Lawlor

11/21/19

Project Writeup Draft

For our project, we have decided to examine the inner workings of a rootkit to understand it, infect a VM with it and do some analysis on it. We also took the original rootkit code and added some more functionality to it. For our rough draft, we have taken the code of a rootkit and done some analysis. While we went through the code to get a better understanding, we made comments to explain the basics of how our rootkit functions. We are in the process of adding new functionalities to the rootkit as well. This project helped us gain a much better understanding of the inner workings of the linux operating system, as well as how rootkits work. This project also expanded our knowledge on writing kernel modules and manipulating devices.

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.