Prof. Dr. C. Eckert
Tamas Lengyel
Fatih Kilic
Thomas Kittel
Sebastian Vogl

Rootkit Programming
WS 2014/2015

Institut für Informatik
Lehrstuhl für
Sicherheit in der Informatik

Assignment 5: Code Hiding

10.11.2014

1 Code Hiding (submitted)

In this assignment the task will be to hide kernel code. This can be achieved by loading a module and hiding that module. It can also be achieved by loading a module that loads your code somewhere else in kernel memory and is then unloaded. Specifically, your module should not show up in `/sys/module` or in the output of `lsmod`.

For the purposes of this assignment, this code should hook the read system call and if the user types "ping" your rootkit should respond with "pong" in the kernel log. There is one additional requirement: Your code should be *cleanly unloadable*. That is, there should be a mechanism by which we can unload your code. The easiest way to do this is to again hook the read system call and look for a specific command that is typed to unload the code.