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 7: Network Keylogging, Command and Control & Privilege Escalation

24.11.2014

1 Network Key-logging (submitted)

Hook the read system call and output the intercepted data when reading from `stdin`. Make sure you also include either terminal and/or PID information such that multiple sessions can be held separate. This output should be printed via UDP packets using the syslog protocol to a syslog-ng server. The UDP packets may be created and sent using the netpoll kernel API.

2 Command and Control (submitted)

Combine file hiding, process hiding, module hiding, and socket hiding into a single root kit. Use a covert communication channel to control the various aspects and what is hidden. That is, which files, processes, modules, and/or sockets are hidden should be controlled through the covert communication channel and *not* when the module is loaded.

3 Privilege Escalation (submitted)

Add a command to the covert communication channel described in Section 2 that escalates the current privileges to root. This can be done by manipulating the current user or shell (or by some other creative method). The method is not important, the result is.