Prof. Dr. C. Eckert
Julian Kirsch
Thomas Kittel
Jonas Jelten

Institut für Informatik
Lehrstuhl für
Sicherheit in der Informatik

Assignment 9: System Call Hooking Revisited & Port Knocking

15.12.2015

1 System Call Hooking Revisited (submitted)

We consider the system call hooking mechanism again: Most of you obtain the base address of the system call table by reading the `sys_call_table` from the `System.map` file. Relying on the presence of this file is problematic in context of generality of your rootkit.

In this assignment you should modify your system call hooking process to not rely on the presence of the `System.map` file anymore. Find a way to derive the base address of the system call table from the (binding) state of the hardware.

2 Port Knocking (submitted)

Port knocking is a method for making TCP servers less visible on the Internet. The basic idea is to make a TCP server not respond (positively) to a TCP SYN request unless a special knock packet has been received first.

Write a machanism that can be used to enable port knocking on any listening TCP socket. The particular design (and the complexity) of the knock packet is up to you. (We shamelessly refer to TCP Stealth[1] for your inspiration.)

3 Infect! (submission 12.01.2016)

Provide a virtual machine image and a snapshot where your rootkit is loaded for the other teams to analyze. To make the analysis more interesting and to ensure that your rootkit actually does something your snapshot should fulfill the following requirements:

- Hide a process that provides a remote shell to you.
- Hide the network connection to the remote shell and make sure it only accepts connections when you politely knock beforehand.
- Enable keylogging to a server of your choice such that you can see what the other teams are doing (and steal their passwords, of course!)

All of this functionality should be enabled when you take your snapshot! We will provide more detailed information next week, this text is just here to make sure everybody gets a heads up before leaving into the (deserved?) christmas vacation.

[1] `https://gnunet.org/kirsch2014knock`

Submission

Generally, put *all* files you want to submit into *one* `.tar.gz` file and submit it on `praksrv.sec.in.tum.de` using the `submit` script. Put all files from one assignment into *one* file!