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

Institut für Informatik
Lehrstuhl für
Sicherheit in der Informatik

Assignment 10: Preparation of the Virtual Machines

22.12.2015

1 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!)
- Make sure your rootkit provides a (secret?) *unloading* mechanism as unloading other teams' rootkits will be part of the next assignment

All of this functionality should be enabled when you take your snapshot! Simply tar up (`tar -czf`) a VirtualBox snapshot (disk *and* memory) of your (i.e. *do not* use the dedicated VirtualBox export functionality") rootkit VM that is booted into a fully functional `root` shell.

Important:

- Your VM Disk Image should be 5 GB max.
- The VM should have only 1024 MB RAM.
- The used kernel must be the same that you created to build your rootkit (see Assignment 1).
- Run `make clean` on your kernel sources to help save space. (Note that the .running kernel must still be buildable from the sources you supply in the VM.)
- For a complete snapshot we need an a `.sav` plus a `.vmdk` file from you.

2 Documentation (submission 12.01.2016)

Create a writeup that describes your rootkit and its functionality:

- What functionality does your rootkit provide?
- How do you achieve this functionality?
- What measures did you take to hide your rootkit?
- How could it be detected?
- How does your unloading mechanism work?

Submission

Submit your writeup, the source code of your rootkit, the VM, and the snapshot to us till 4pm on the 12th of January. 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* archive!