Keylogger/Backdoor Rootkit

Winter term 2015/16

Applied Information Security

Clemens Brunner
Michael Fröwis

January 5, 2016

Contents

1 Introduction **3**
1.1 Kernel Modules 3
1.2 Kernel Rootkits 3

2 Implementation **3**
2.1 Keylogging 3
2.2 Backdoor 3
2.3 Hiding 3
2.4 Networking and Activation 3
2.4.1 ICMP Packages 4
2.4.2 UPD Sockets 4

3 Conclusion **4**

1 Introduction

In the following we want to explore how to make a linux kernel rootkit. As the definition of a rootkit stats it should run as root and should be hard to detect for users. To give the rootkit real value it has to do something. We decided to go with two very common usecases when it comes to

1.1 Kernel Modules

1.2 Kernel Rootkits

2 Implementation

2.1 Keylogging

This section deals about keylogging in linux kernel. Keylogging describes the process of intercepting all inputkeys from a keyboard. Our rootkit intercepts all keys and sends them to a server. It is possible to activate and deactivate the keylogging function with a magic package, see 2.4. To implement a keylogger in the linux kernel you must register a keyboard notifier.

```
register_keyboard_notifier(&keyboard_notifier);
```

The keyboard notifier stores the keyboard_hook method which will be called on each key press. This function gets a keyboard keycode as input, to filter out the associated character we use two arrays with the mapping for the american keyboard layout. The first one is the mapping without SHIFT and the secound is with SHIFT pressed.

2.2 Backdoor

2.3 Hiding

2.4 Networking and Activation

To communicate with the rootkit two methods are used.

- ICMP Packages
- UDP Sockets

2.4.1 ICMP Packages

To activate the keylogger, hide the rootkit modul or open a backdoor shell with root access magic packages are used. We used a normal ping package where the code is the same as the id. The following values are used for code and id to assign the descriped functionality.

122: KEYLOGGER_ACTIVATION_CODE

123: KEYLOGGER_DEACTIVATION_CODE

124: HIDEMODULE_ACTIVATION_CODE

125: HIDEMODULE_DEACTIVATION_CODE

126: BACKDOOR_ACTIVATION_CODE

To catch the packages a new netfilter_hook is added with the netfilter libary.

```
nf_register_hook(&netfilter_hook);
```

The netfilter hook catches all icmp packages for the evaluation only packages the already defined properties are used.

2.4.2 UPD Sockets

For sending the keys to the client and for controlling the server with the backdoor shell, UPD datagram packages are used.

3 Conclusion