Rootkit Rootkit: Keylogger/Backdoor

Clemens Brunner Michael Fröwis

clemens.brunner@student.uibk.ac.at michael.froewis@student.uibk.ac.at

January 19, 2016

Introduction

Kernel Modules

Implementation

Hiding

Backdoor

Keylogging

Networking and Activation

Livedemo

Introduction Kernel Modules

Implementation

Hiding

Backdoor

Keylogging

Networking and Activation

Livedemo

Introduction

- General: Rootkit
 - Software
 - Root privileges
 - Masking existence
- Our tool: Linux kernel rootkit
 - Keylogging
 - Backdoor

Introduction: Kernel Modules

- Kernel Modules
 - No rebuild
 - No reboot
- Example:

```
#include <linux/module.h>
2
    #include <linux/kernel.h>
    int init_module(void){
5
6
             printk(KERN_INFO "Hello_world_1.\n"):
             return 0:
8
    void cleanup_module(void){
9
             printk(KERN_INFO "Goodbye_world_1.\n");
10
11
12
    module_init(init_module):
13
    module_exit (cleanup_module);
14
15
    MODULE_LICENSE("GPL");
```

```
Introduction
```

Kernel Modules

Implementation

Hiding

Backdoor

Keylogging

Networking and Activation

Livedemo

Hiding

- Mask existence
 - Kernel modules not visible as a process
- lsmod
 - special exported symbol extern struct module __this_module;
 - list_del (&(__this_module. list));

```
1  struct module {
2   enum module_state state;
3   
4     /* Member of list of modules */
5     struct list_head list;
6     /* Unique handle for this module */
8     char name[MODULE_NAME_LEN];
9     ..
10     // skipped for brevity
11 }
```

Backdoor

- Spanning userland process
 - \circ netcat -l -p 6666 -e /bin/sh
 - o call_usermodehelper

backdoor.c

Keylogging

- Linux Kernel provides function
 - Register a struct notifier_block keyboard_notifier
- keyboard_hook gets keycode as input
 - $\circ \ \, \mathsf{Mapping:} \ \, \mathsf{Keycode} \to \mathsf{Character} \, (\mathsf{US})$

Networking and Activation

- Magic Packet
 - \circ Ping Request where ID == Code
 - o Used codes: 122 126
 - Nethook API
- Sending key characters
 - UDP datagram socket

Introduction

Kernel Modules

Implementation

Hiding

Backdoor

Keylogging

Networking and Activation

Livedemo

Livedemo

Demo...

Introduction

Kernel Modules

Implementation

Hiding

Backdoor

Keylogging

Networking and Activation

Livedemo

Summary

• Simple rootkit: easy

• Perfect rootkit: very hard

Bibliography

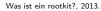


Dan Goodin.

Gpu-based rootkit and keylogger offer superior stealth and computing power, 2015.



Serge Malenkovich.





Morgan Phillips.

How to: Building your own kernel space keylogger, 2014.



Unknown. How to: Building your own kernel space keylogger, 2010.



Unknown.

Kernelmode rootkits: Part 3, kernel filters, 2014.



Unknown.

Part 1: Stealing keyboard keys for fun profit, 2014.