Linux rootkits & TTY Hijacking

Antonio Pérez Pérez <antonio.perez.perez@cern.ch>
CERN Computer Security Team

EGI Technical Forum 2011, Lyon, France

Outline

- Rootkits: Introduction
- Linux rootkits
  - History
  - Detection and monitoring
  - Removal
- TTY Hijacking
  - Introduction
  - How it works
  - What does it mean?
  - Mitigation?

Rootkits: Introduction

"A rootkit is a collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network" (whatis.com)

"Designed to hide or obscure the fact that a system has been compromised" (Wikipedia)

Set of software to maintain malicious access to a compromised host

Types:

- User mode
- Kernel mode
- Hypervisor level
- Firmware

CERN IT
Department
CH-1211 Genève
23
Switzerland

Rootkits: Introduction (cont.)

Common functions:

- Hide processes
- Hide files
- Hide network sockets
- Backdoor
- Keylogger

CERN IT
Department
CH-1211 Genève
23
Switzerland

Linux rootkits

User-mode rootkits

Overwrite system binaries/libraries

- Change binaries (netstat, du, ping, lsof, ssh) or libraries (ld.so.preload, etc)
- Kernel independent
- Need to be compiled for the platform, easy to detect

How to detect: checking system binaries against trusted sources/instances

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Kernel-mode rootkits

Kernel-mode rootkits

- Malicious code is loaded directly in the kernel
- Direct /dev/{k,}mem access (patch kernel on-the-fly)
- Difficult to detect, usually includes backdoor features
- LKM may be disabled, access to /dev/{k,}mem may be restricted

How to detect: search for known patterns, or known bugs

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Kernel-mode rootkits

Flow of control on a system call:

1. An interrupt is triggered, and execution continues at the interrupt handler defined for that interrupt. On Linux, interrupt 80 is used

   A rootkit could replace the kernels interrupt handler by an own function. This requires a modification of the Interrupt Descriptor Table (IDT)

2. The interrupt handler (system_call()) looks up the address of the requested syscall in the syscall table, and executes a jump to the respective address

   A rootkit may (a) modify the interrupt handler to use a (rootkit-supplied) different syscall table, or (b) modify the entries in the syscall table to point to the rootkits replacement functions

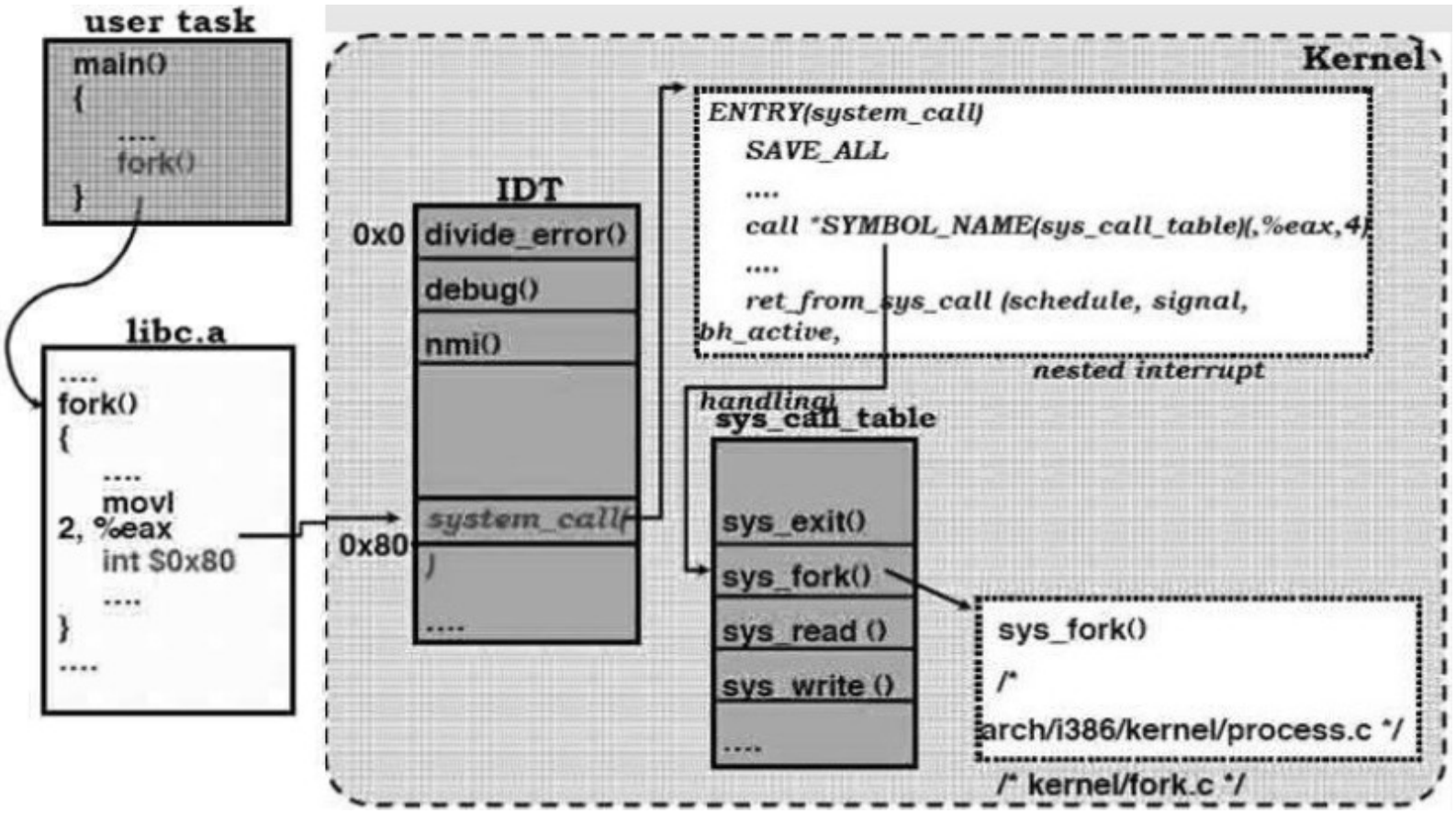
3. The syscall function is executed, and control returns to the application

   A rootkit may overwrite the syscall function to place a jump to its own replacement function at the start of the syscall function

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Kernel-mode rootkits



CERN IT
Department
CH-1211 Genève
23
Switzerland

Example of kernel-mode rootkit

SucKIT

- Presented in Phrack issue 58, 0x07
- Fully working rootkit that is loaded through /dev/kmem
- No need for LKM support
- Modifies the interrupt handler to use a (rootkit-supplied) different syscall table
- Provides a password protected remote access connect-back shell initiated by a spoofed packet, and can hide processes, files and connections

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

New trends

Filesystem, network stack level rootkits

- Often used as additional features

Hypervisor rootkits

- The OS within the rootkit
- Example: Subvirt

Debug Register based rootkits

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Detection and monitoring

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Detection and monitoring

There is no unique (or simple/magic) solution: combination of different tools

Monitoring filesystem binaries/libraries:

- tripwire
- rpm -V
- ...

Looking for known patterns or bugs:

- rkhunter
- chkrootkit
- Samhain
- ...

CERN IT
Department
CH-1211 Genève
23
Switzerland

Data integrity tools

Tripwire

- Detects changes on the filesystem level
- Scans the file system and stores information on each file scanned in a database. The results compared against the stored values in the database

rpm -V | --verify

- Available on RPM-based distributions
- Compares information about the installed files in the package with information about the files taken from the package metadata stored in the rpm database

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

rkhunter

Scans for rootkits, backdoors and local exploits by running tests like:

- MD5 hash compare
- Look for default files used by rootkits
- Wrong file permissions for binaries
- Look for suspected strings in LKM and KLD modules
- Look for hidden files
- Optional scan within plaintext and binary files

CERN IT
Department
CH-1211 Genève
23
Switzerland

chrootkit

Tool to locally check for signs of a rootkit

Checks:

- system binaries for rootkit modification
- if the network interface is in promiscuous mode
- for lastlog, utmp and wtmp deletions
- signs of LKM trojans
- quick and dirty strings replacement.

CERN IT
Department
CH-1211 Genève
23
Switzerland

Host Intrusion Detection Systems

samhaim

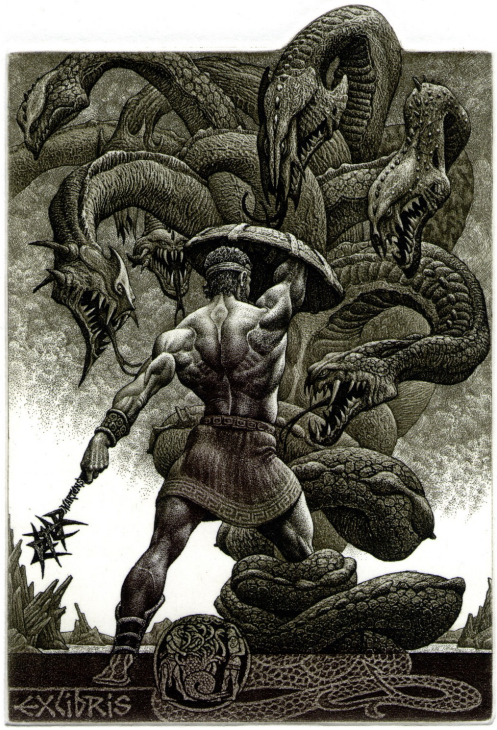
Provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Removal

Usually there is no easy removal method



Clean reinstall is highly recommended!

TTY Hijacking

Introduction

- Way for an attacker to take over a user's session
- Requires root privileges
- Old known technique gaining more attention lately as it's getting added as feature on rootkits

CERN IT
Department
CH-1211 Genève
23
Switzerland

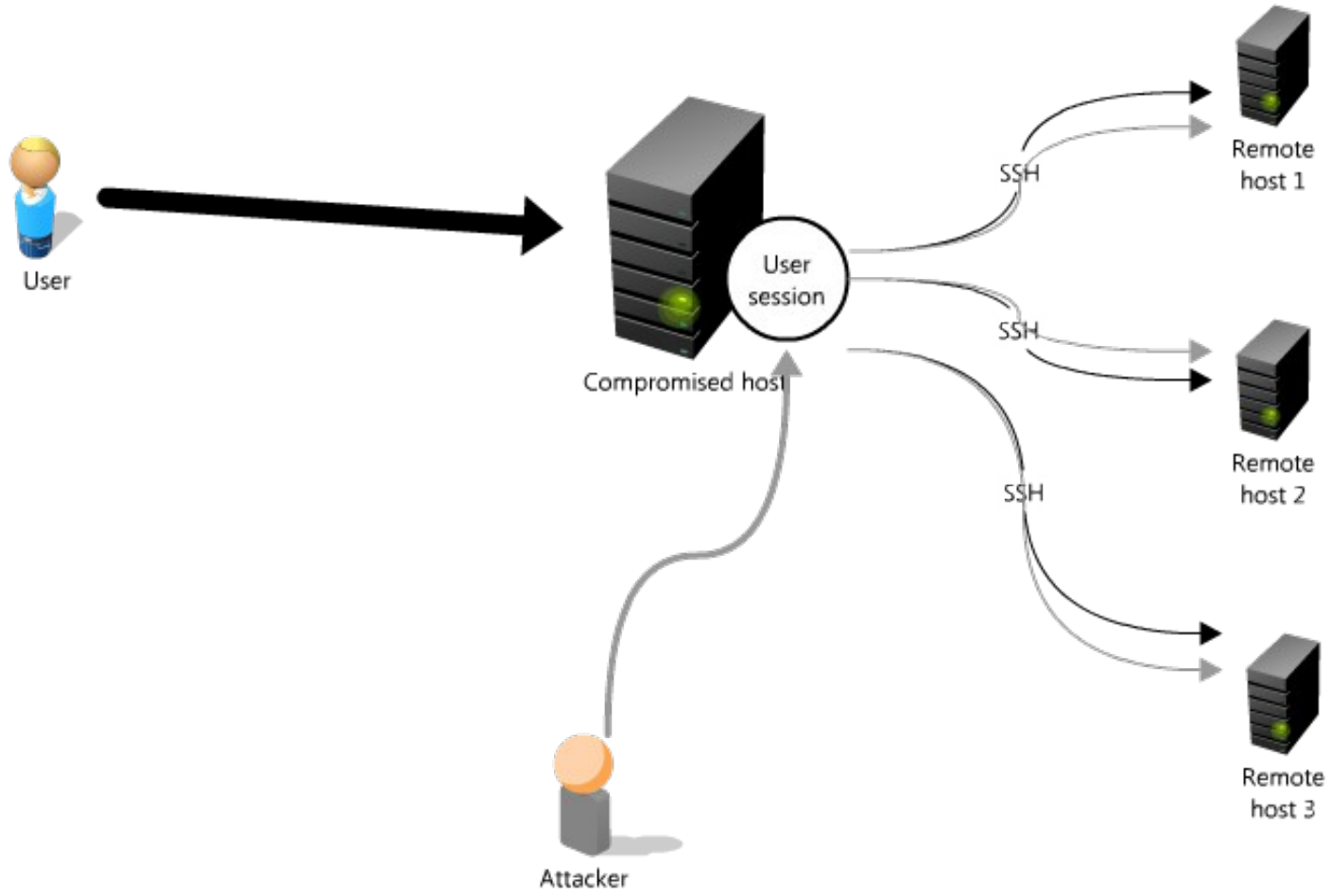
How it works

1. Attaches to the victim's session
2. Redirects the write() system call to the attacker's code which logs the contents of the write if it is directed at the tty; it can then call the real write() system call
3. Profit!

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

How it works (cont.)



CERN IT Department
CH-1211 Genève 23
Switzerland

What does it mean?

If a rootkit implements TTY Hijacking features, all legitimate connections made on a compromised host can be intercepted by the attacker and act as a gateway to new hosts

Doesn't matter if the attacker doesn't have the user credentials on the remote hosts (password or ssh keys)

The session hijacking can be hidden completely to the victim

Department Infrastructure

CERN IT Department
CH-1211 Genève 23
Switzerland

Mitigation?

TTY Hijacking on a compromised (rooted) host means you were already screwed from the beginning

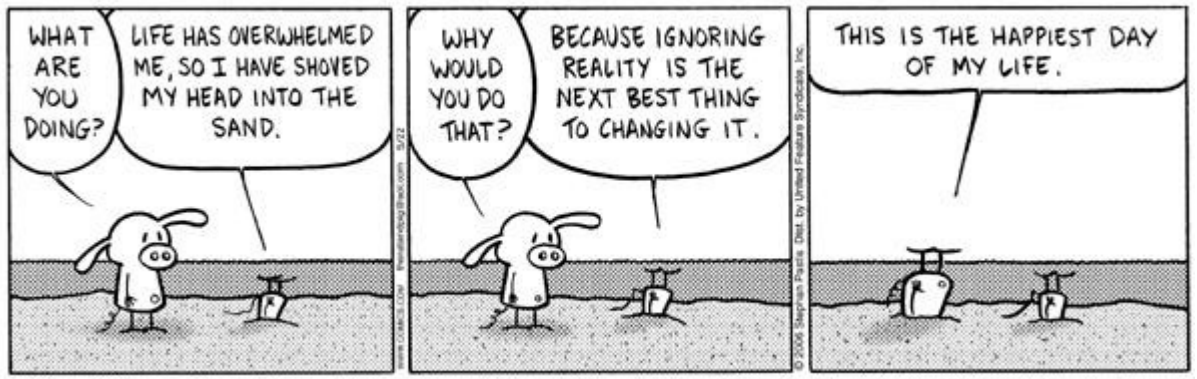
CERN IT
Department
CH-1211 Genève
23
Switzerland

Conclusions

Defending against rootkits is always an ongoing work. Rootkits are getting more and more sophisticated

There isn't a magic tool that detects everything. Use combination of them for better results

TTY Hijacking is “just” a feature added on rootkits. Mitigate the root of the problem


WHAT ARE YOU DOING?
LIFE HAS OVERWHELMED ME, SO I HAVE SHOVED MY HEAD INTO THE SAND.
WHY WOULD YOU DO THAT?
BECAUSE IGNORING REALITY IS THE NEXT BEST THING TO CHANGING IT.
THIS IS THE HAPPIEST DAY OF MY LIFE.
© Stephan Pastis/Dist. by UFS, Inc.

Questions?