Linux Systems

Compromised

Understanding and dealing with break-ins

Michael Boelen
michael.boelen@cisofy.com

Ede, 5 February 2016
Agenda

Today

1. How do “they” get in
2. Rootkits
3. Malware handling
4. Defenses
Michael Boelen

- **Security Tools**
  - Rootkit Hunter (malware scan)
  - Lynis (security audit)
- 150+ blog posts
- Founder of CISOfy
How do “they” get in
Intrusions

- Passwords
- Vulnerabilities
- Weak configurations
Why?
Keeping Control

● Rootkits
● Backdoors
Rootkits 101
Rootkits

- (become | stay) root
- (software) kit
Rootkits

- Stealth
- Persistence
- Backdoors
How to be the best rootkit?
Hiding ★

In plain sight!

/etc/sysconfig/…
/tmp/mysql.sock
/bin/audiocnf
Hiding ★★

Slightly advanced

- Rename processes
- Delete file from disk
- Backdoor binaries
Hiding ★★★

Advanced

- Kernel modules
- Change system calls
- Hidden passwords
Demo
Demo

```
[root@centos tmp]# ls -l
total 384
-rw-r--r--. 1 root root 390521 Feb 3 12:31 backdoor.ko
[root@centos tmp]# insmod backdoor.ko
[root@centos tmp]# lsmod | grep backdoor
[root@centos tmp]# ls /proc | grep backdoor
[root@centos tmp]# ls -l
total 0
```
Demo

```
[root@centos tmp]# ls -l
total 0
[root@centos tmp]# touch hideme
[root@centos tmp]# ls -l
total 0
-rw-r--r--. 1 root root 0 Feb 3 12:36 hideme
[root@centos tmp]#
[root@centos tmp]# touch HIDEme
[root@centos tmp]# ls -l
total 0
-rw-r--r--. 1 root root 0 Feb 3 12:36 hideme
```
Continuous Game
Detection
Challenges

● We can’t trust anything
● Even ourselves
● No guarantees
Rootkit Hunter

Detect the undetectable!
Dealing with malware
Activate your plan!

- Owner?
- Risk?
- What if we pull the plug?
Quarantine

VLAN

Bogus DNS

Looks Real™
Consider Research

Memory dump
(Volatility)

Static analysis
Restore

Does it include malware?
Defense
Best protection

At least

● Perform security scans
● Collect data
● System Hardening
Frameworks / Patches

- SELinux
- AppArmor
- Grsecurity
Compilers

- Remove
- Limit usage
Harden Applications

● Use chroot
● Limit permissions
● Change defaults
Kernel Hardening

- sysctl -a
- Don’t allow ptrace
Automation
Tip: Lynis

- Linux / UNIX
- Open source
- GPLv3

```text
[+] Users, Groups and Authentication
---------------------------------------------------
- Search administrator accounts...                   [ OK ]
- Checking UIDs...                                   [ OK ]
- Checking chgrp tool...                             [ FOUND ]
- Consistency check /etc/group file...               [ OK ]
- Test group files (gpgc)...                        [ OK ]
- Checking login shells...                           [ WARNING ]
- Checking non unique group ID's...                 [ OK ]
- Checking non unique group homes...                [ OK ]
- Checking PAM authentication support              [ NOT ENABLED ]
- Check /etc/sshauthers file                        [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Shells
---------------------------------------------------
- Checking console TTYs...                           [ WARNING ]
  - Checking shells from /etc/shells...
    Result: Found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] File systems
---------------------------------------------------
- [FreeBSS] Querying UFS mount points /fstab...     [ OK ]
  - Query swap partitions /fstab...                 [ OK ]
  - Testing swap partitions...                     [ OK ]
  - Checking for old files in /tmp...              [ WARNING ]
  - Checking /tmp sticky bit...                    [ OK ]
```
Conclusions
Conclusions

- Good rootkits are hard to detect
- Use cost-effective methods
  - Detect
  - Restore
  - Learn
- Apply hardening
Success!

You finished this presentation
More Linux security?

Presentations
michaelboelen.com/presentations/

Follow

● Blog  Linux Audit  (linux-audit.com)
● Twitter  @mboelen