Erste Hilfe in Digitaler Forensik

Dirk Wetter @
Dr. Wetter IT-Consulting, (http://drwetter.de)

Hamburg

Secure Linux Administration Conference 2, Berlin, 6.-7.12.2007

Agenda

I. Einleitung

II. Begriffe + Arbeitsweise

III. Verdacht erkennen + erhärten

IV. Beweissicherung

V. Vorbeugen ist besser als ...

Um was geht's?

- Incident Response d. CF = bis vor P.M.-Analyse
- Methodik
- Handwerkszeug Kommandozeile
- Beschränkung auf
  - PC-Hardware
  - Linux
  - Verwendung von OSS
- einfache Problemstellung
  - kein RAID, DB, ATA-HPA/DCO, -SE
  - keine Tatortsicherung

Digitale / Computer-Forensik

- Unterscheidet:
  - Live-Forensik
  - Post-Mortem-Forensik
- Wort „Forensik“ bestimmt Arbeitsweise

Forensik allgemein

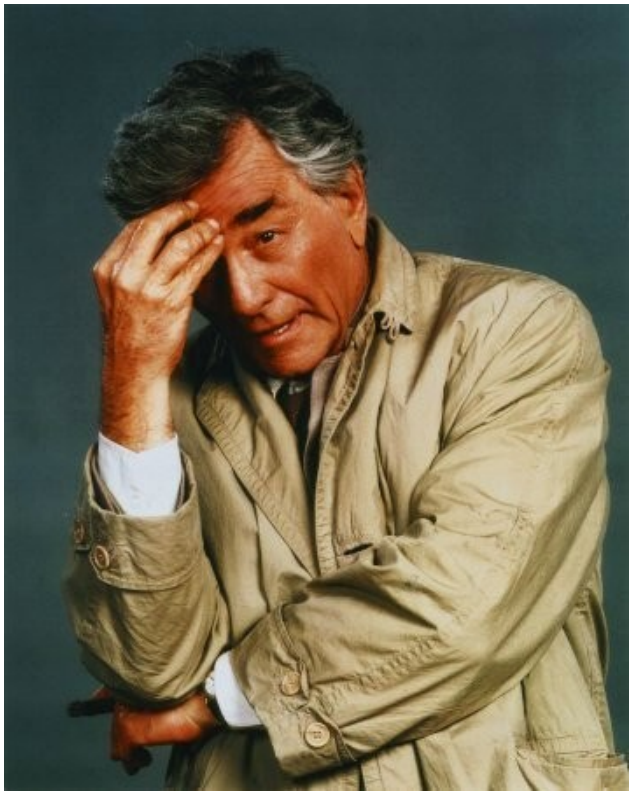
- Wikipedia:

  „Unter dem Begriff Forensik werden die Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen identifiziert, analysiert oder rekonstruiert werden.“

  - systematisch
  - kriminell
  - identifizieren
  - analysieren / rekonstruieren

Schlussfolgerung

- Es geht um *Digitale Beweise*
- gerichtliche Verwertbarkeit
- Zum Zeitpunkt der Entdeckung:
  - kein Wissen über Täter
    - intern / extern
    - Motivation
  - Schaden



Locards Austauschprinzip

Jeder und alles am Tatort nimmt etwas mit und lässt etwas zurück.

Freistellungsauftrag ;-)

- **Disclaimer**: Ich bin kein Anwalt

Umgang mit Beweisen

- sorgfältig!
  - Flüchtiges zuerst sichern
  - Dann Nicht-Flüchtiges
  - kein Zerstören
  - sicheres Aufbewahren
  - **Dokumentieren! (Wer, wann, was, wo, wie)**

Dokumentation, Hintergrund

- **Beweiskette** für Gericht
  - Strafverfahren
  - Zivilansprüche
- Nachvollziehbarkeit für Nicht-Profis
- vier Augen beweisen mehr ...
- Gerichtsfestigkeit:
  - Versetzen in die Rolle des Beschuldigten/Angeklagten

Dokumentation, technisch

- **„5 x W“: Wer, Wann, Was, Wo, Wie**
- digital:
  - `date(1) [2x]`
  - `script(1), screen(1): log*`
  - Prüfsummen
- nicht digital
  - Zeit,
  - Unterschrift,
  - Seitennummerierung (Lückenlosigkeit)

Handlungsweise

- Einen **Plan/Strategie** haben (ggf. machen!)
  - Firma (Sicherheitsrichtlinien, Notfallkonzept)
  - technischer Ablaufplan

Firma: CERT

- Notfallkonzept
  - Organisatorisch (Meldung, Handling)
  - Betrieb + Verfügbarkeit
  - Umgang mit personenbezogenen Daten + Betriebsgeheimnissen während IR
- BSI-Grundschutzhandbuch/-kataloge
  - B 1.3, B 1.8: Notfallvorsorge-Konzept, Behandlung von Sicherheitsvorfällen
  - M 6: Maßnahmenkatalog

Kleine Lehre d. Versteckens

- erstes RK: 1990 für SunOS 4.1.1
- Rootkit manipuliert:
  - Prozesse
  - Verzeichnisse, Dateien (Binär, Libs)
  - Sockets
  - Log-Manipulation
  - Speicher
- Meistens: Hintertür zur Fernsteuerung
  - automatisiert!

Artenvielfalt Rootkits

A) häufig Kernel-RK:

- Kernel-Modul
- Umlenken syscalls –> Sichtbarkeit Netz, Dateien
- wenig im Dateisystem zu finden

B) seltener reines User-Level-RK

- mehr Spuren

C) Fies: *in-memory* Rootkits (=*non-persistent*)

Anomalien

- Erkennung nicht trivial
  - IDS (Host, Netzwerk)
  - Log-Meldungen
    - Tageszeiten
    - fehlende
    - Art
  - Netzwerkverbindungen (Peers, Anzahl)
  - „komische“ Prozesse, Dateien
  - Statusveränderungen (PROMISC, fehlerhafte/fehlende Dateien)

Netz: minimal invasiv

- Mirror Port
- „Hubbing out“
- Mithorchen „in der Mitte“
  - Firewall-, Routermitschnitt
  - `ettercap` (MITM)
- Problem:
  - Tageszeit des Netzwerkverkehrs
  - Verschlüsselung

Am System: invasiv

- Ziele bei P.M.-Analyse
  - Auffinden gelöschter Dateien
    - evtl. Löschdatum
  - Timeline-Analyse:
    - Rekonstruktion: wann was passiert ist
    - atime, mtime, ctime
  - ...

→ Jeder Zugriff ab nun (Erhärtung/Duplizierung) zerstört u.U. Beweise!

Am System: Vorsicht...

- ... ist die Mutter des Forensikers
  - ~~`find / | xargs strings h8ckm3 >/sbin/datei.log`~~
  - `mount -o remount,noatime <dir>`
  - evtl. `killall hald`
  - Separation im Netz
  - Nicht herunterfahren!
- Vertraue dem System nicht
  - Binaries
  - Libs
  - Kernel

→ Externe Tools!

- statisch gelinkt:

```
hacked:/mnt/Static-Binaries/linux_x86 0# ldd uptime
        not a dynamic executable
hacked:/mnt/Static-Binaries/linux_x86 1# file uptime
uptime: [...], statically linked, stripped
```

- woher?
  - CD/DVD (manipuliersicher)
  - USB-Stick (-Platte)
  - kopiertes Verzeichnis
  - falls vorhanden und eingehängt:
    - NFS, CIFS, AFS

Womit?

- Helix:
  - www.e-fense.com/helix (GPL)
  - Drei Zwecke:
    - Beweis erhärten
    - Volatile Daten sichern
    - P.M.-Forensik
  - keine Solaris-Bins mehr (Windows: ja)
  - `procget`, `pcat`, `pd`
  - evtl. selbst erweitern!

Anfang der Suche

- schön wäre: `bash --noprofile --norc`
- `mount <Helix-CD> /mnt`
- `PATH=/mnt/Static-Binaries/linux_x86; HISTFILE=/dev/null`
- `unset LD_LIBRARY_PATH (LD_PRELOAD)`
- `lsof (-i) -Pn / netstat -atupn`
- `last -aix / who -a / ps -efwly`
- fehlt MARK im Syslog (läuft Dämon?), `dmesg` anschauen
- `ls -la /root/.*history*` (Länge Null? Link `/dev/null`? Anschauen!)
- `ls -la /home/*/.*history*`, u.a. Benutzer wie `www-*`
- `ifconfig | grep PROMISC`
- `ls -ulrt / ls -lrt`

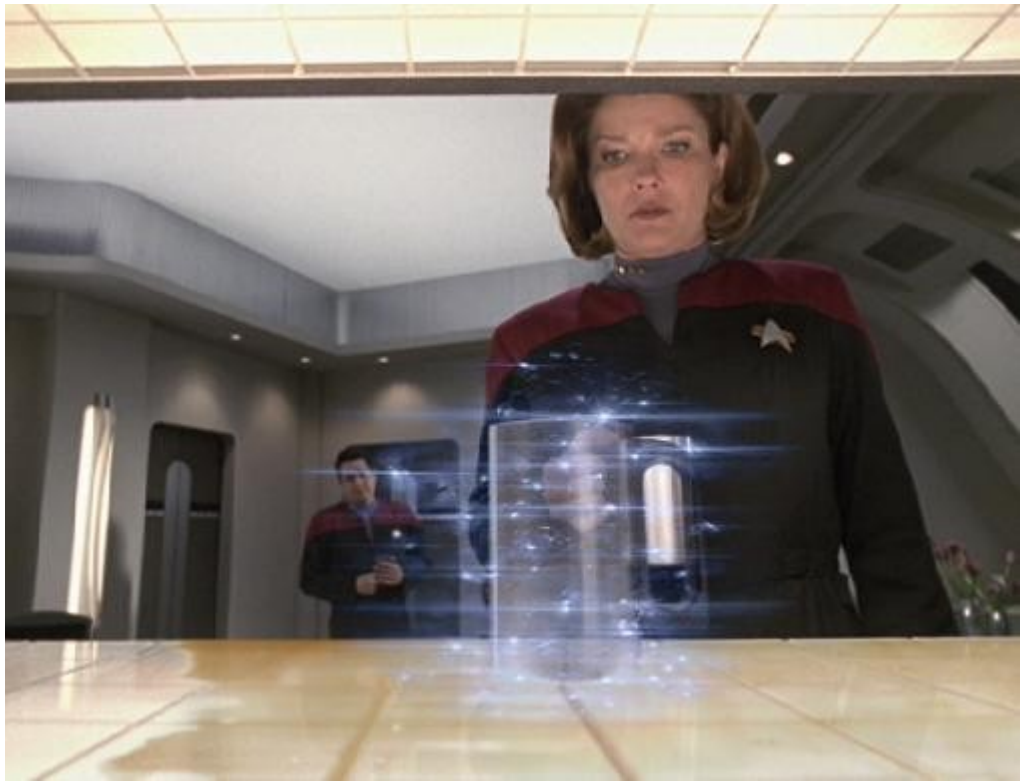
Nützlich

- `/bin/rpm -Va` (nicht auf Helix-CD, noatime-Mount!)

  (`debsums -s` für Debian-Dialekte)
- beides lokale DB: Nur Anhaltspunkte

- Log-Dateien im Netz:
  - Proxy
  - IDS, IPS
  - Mail
  - Firewall, Router, Switch, Netflow
  - „Seuchengefahr“: Scan des Intranets (Inter-)

- ok. Jetzt weiß ich: Rechner ist kompromittiert.
- Und nun?



- CERT involvieren
- Daten sichern
  a) Flüchtige Daten
  b) Rechner außer Betrieb
  c) Forensisches Duplikat

a. Vorgehensweise

- i.e. „Dead Acquisition“

- Prinzipiell auch möglich:
  - Erst forensische Duplikation
  - Dann außer Betrieb
  - „Live Acquisition“

→ Bietet sich an bei nicht-gängigen Platten/HBAs

→ Skepsis wegen Kernel

Beweissicherung

- nicht überstürzt
- Beweishandhabung!

It looked insanely complicated, and this was one of the reasons why the snug plastic cover it fitted into had the words DON'T PANIC printed on it in large friendly letters. The other reason was that this device was in fact that most remarkable of all books ever to come out of the great publishing corporations of Ursa Minor - **The Hitchhiker's Guide to the Galaxy**.

Wie?

- Anzahl Kommandos
- Ausgaben:
  - Stempel korrektes Datum (Tag+Uhrzeit)
  - „Hinreichende“ Prüfsummen (`md5sum`, `sha1(deep)`, `sha256deep`)
- Tools:
  - Helix-CD (USB)
  - ähnliches bzw. eigener Werkzeugkasten
- Skepsis

Wie?

- Vorsicht Helix: `linux-ir.sh`
  - überflüssigerweise nicht-flüchtige Daten
  - atime (`remount,noatime ; killall hald`)
- besser, nicht ganz perfekt:
  - iX 7/2007: http://computer-forensik.org/tools/ix/
  - oder: http://software.drwetter.de/ir/

Was alles? (Plan)

- RAM
- Anderes Flüchtiges wo Neustart=Verlust
  - Info + Status
  - Verschlüsselte Dateisysteme (!)
  - (ggf. Swap)

Wohin?

- USB/Firewire (ext. Platte, -Stick: /dev/kcore)
  - Einfach
  - Sicher (well,...)
  - Zugänglichkeit
- Netz

Netz

- netcat: „Schweizer Forensikmesser I“
  - `fws:/forensik/case1 0# netcat -lp 42 >datei.txt`
  - `hacked:~ 0# cat /proc/version | netcat fws 42`
  - Nachteil:
    - Empfänger weiß nichts von Senderdateiname
    - `netcat`: unverschlüsselt/-authenifiziert
    - besser:
      - `cryptcat (-k passphrase)` (Blowfish)
      - `socat`: sehr mächtig, x509-Key-Auth sinnvoll
      - [`sbd`, `aes-netcat`, `ncat` (Proxy, AES, ...)]

Wie?

- **`date`** (Uhrzeit/Datum korrekt?)
- `PATH=/mnt/Static-Binaries/linux_x86:/usr/bin:/bin:/sbin:/usr/sbin`
- `HISTFILE=/dev/null`
- `unset LD_LIBRARY_PATH LD_PRELOAD`

- Platte: `df -kT`, `mount -l`, `pv/vg/lvdisplay`, `mmls`
- Prozesse: `ps -eflwy`, `lsof -Pn`, `top -bn1`
- Netz: `ifconfig -a`, `arp -a`, `arp -n`, `netstat -atunp`, `lsof -i -Pn`, `iptables-save`
- Status: `uptime`, `dmesg`, `sysctl -A`, (evtl. `who`, `last`)

Was alles?

- `/dev/kcore` (`memdump` (tct), `memget`, `mempeek`)
- `/proc`:
  - `modules`, `cmdline`, `version`, `kallsysms`,`swaps`, `mount`, `devices`, `uptime`, `diskstats`, `misc`, ...
  - jeden einzelnen Prozess: `/proc/[0-9]*/*` (`pd`, `pcat`)
- geht immer & spart Platz: `gzip -c`
- ggf.: Krypto-Dateisysteme sichern
- Prüfsumme(n) und Datum nicht vergessen!

Generelles

- Runterfahren:
  - Fasst Hunderte von Dateien an (atime)
  - Modifiziert nicht wenige (*.pid, *log, ..)
  - Unvorhersagbar: Reallozierung Platz gelöschter Dateien
- Ausschalten:
  - Dateisysteme unsauber (erschwert stellenw. Analyse)
  - Durch **Netzstecker**, nicht „Power“-Knopf!
  - ggf: SYSRQ-[S,S,U,B*] (ggf `sysctl -w kernel.sysrq=1`)
  - SYSRQ-[T,M,P] via Konsole

*) Vorsicht: wg. Reboot, ggf geht O statt B

d. Forensische Kopie

- In-situ (am Objekt)
  - Viel Daten = lange Wartezeit
  - 100 GB = 27 h bei 100 Mbit/s / langsame USB-Platte
- Ex-situ
  - Platte (=Beweis) ausbauen+mitnehmen
  - In Ruhe forensisches Duplikat erstellen
  - Schreiben unter allen Umständen verhindern
  - (Profis: Write-Blocker)
- Original unter Verschluss

Was?

- Die ganze Platte!
- Nicht partitionsweise
- Lücken, (absichtlich) unbenutze Bereiche

- Beispiel aus dem Leben (`mmls`)

Was?


```
fws:~ 0# mmls /dev/sdb
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
[...]
21:  -----   0196780186   0196780247   0000000062   Unallocated
22:  07:00   0196780248   0213552044   0016771797   Linux LVol.Manager (0x8e)
23:  -----   0213552045   0234441647   0020889603   Unallocated
```

Was?


```
fws:~ 0# fdisk -u -l  /dev/sdb
[...]
/dev/sdb7       186948468   188956529     1004031   82  Linux swap / Solaris
/dev/sdb8       188956593   196780184     3911796   83  Linux
/dev/sdb9       196780248   213552044     8385898+  8e  Linux LVM

Partition table entries are not in disk order

frns-ws:~ 0# dd if=/dev/sdb skip=213552045 count=1 | xxd
1+0 records in
1+0 records out
512 bytes (512 B) copied, 8.1855e-05 s, 6.3 MB/s
0000000: c774 96e1 1ecd 8923 ebea f7bf c737 731c  .t.....#.....7s.
0000010: f83a 195d 9582 b742 63b7 fb2e f20e 17a4  .:.]...Bc.......
0000020: 2eea da92 2202 259c 6f37 fb73 1311 e574  ....".%.o7.s...t
0000030: eaab af2e f66d 488d 8427 25c4 75ba 6e7b  .....mH..'%.u.n{
0000040: f82d fb75 8e87 b180 5245 bb11 afba 5105  .-.u....RE....Q.
[...]
```

Kopie der ganzen Platte

- Frisches Dateisystem auf Sicherungsplatte
- Einhängen (hier `/mnt`)
- **`d=/mnt/mmls_hdX_`date +%F,%T``**
- **`mmls /dev/hdX >$d; $sum $d > $d.$sum`**
- **`$sum /dev/hdX >/mnt/hdX.$sum`**
- **`$dd if=/dev/hdX >/mnt/hdX.img`**
- **`$sum /mnt/hdX.img`** (sollte gleich sein)

- `$sum: md5sum, sha1, sha1deep, sha256deep`

Schweizer Forensik-Messer II

- $dd (disk dump):
  - Standard Blockgröße 512 Bytes ist zu langsam
  - „Standard-`dd`“ (fileutils): `conv=noerror`
  - `sdd` (Schily): „verbessertes dd“, schneller
  - `dd_rescue`: besser bei Lesefehler und Spulen (Kurt Garloff @ Suse)
  - `dcfldd`
    - `-hash=md5|sha1|sha256..sha512` (`-hashlog`), `-status`
  - Forensik Acquisition `dd`:
    - Zeitstempel plus Prüfsumme
    - leider kein Quellcode, Linux-Support?

Mein Favorit (YMMV)

- dcfldd

```
host:~|0% dcfldd if=/dev/urandom of=/dev/null \
   count=768 hash=sha256
256 blocks (8Mb) written.
512 blocks (16Mb) written.
768 blocks (24Mb) written.Total (sha256): 70554677ac031d-
   d45da2b9de6ba3fe8661c8d75af8aa61d65b479f6143284f55

768+0 records in
768+0 records out
host:~|0%
```

andere Werkzeuge

- Eigene „Imager“ (u.v.m.)
  - EnCase (prop. Format)
  - X-Ways Forensics
  - Forensic Tool Kit
- alles Windows-Programme (auch ext3, reiserfs)
- (Linux P.M.-Tools
  - The Sleuth Kit (TSK)
  - The Coroners Tool Kit (TCT, tctutils)

)

Weiteres

- Nun:
  1. Original-Beweis sicherstellen
  2. Post-Mortem-Analyse von der Kopie

- Zeitgleich/danach:
  - Rechner neu aufsetzen
  - Neue Passwörter
  - Konsequenzen aus P.M. schließen

Patches!

- Patch-Policy:
  - Firma
  - Admin
- Cronjobs + Mail für Patchstand:
  - Debian/Ubuntu:
```
apt-get update >/dev/null && \
    apt-get --dry-run upgrade 2>&1
```
  - Suse/SLES: `zypper patches | grep "| Needed"`
  - RedHat/Fedora: `yum update` (`update -u` RHEL2-4)
  - Nicht 4200 Hosts zur selben Zeit ;-)

Handwerkszeug

- KISS:
  - Automatisieren (Installationen, Maintenance, Checks, ...)
  - Wenig „selbstgeb(r)autes“
- Zeitsynchronisation (alle OS): NTP
- Zentrales System-Logging (alle OS)
  - Hacker's worst enemy
  - syslog-ng (Server+Client), `MARK` messages, TCP
  - Bastion-Host für Logs (Backups)

Tipps zur Verhütung

- **zentrales** Host-IDS (file integrity)
  - AIDE, Tripwire von Bastian-Host:
    - Master-DB: Remote (oder CD)
    - Remote Execution (SSH-Key)
  - Weniger ist mehr:
    - SUID-root-Dateien `find / -perm +4000`
    - Eintrittsvektor-Binaries (Server-Dienste)
    - übliche User-RK-Verdächtige: `ps`, `ls`, `netstat`, `ld-linux.so`, `libc`, `top`, `kill(all)` (`lsof`, `strace` ...)
    - wichtige configs u.a.: `/etc/{hosts,shadow, modprobe.conf,ssh/,syslog-ng/, ...}`

„Peter & der Wolf“-Effekt: False Positives

Härten

- für exponierte Rechner/Dienste:
  - Server-Dienste im Sandkasten (MAC):
    - AppArmor
    - SELinux
    - (Jails, Container, RBAC, TX, ...)
  - Applikationsebene
  - XSS, CSRF, Session Riding, Race Cond., File Inclusion
  - z.B. Suhosin, Quellcode-Audit-Werkzeuge
  - `CONFIG_MODULES=n`

Index services

- beagle und Freunde:
  - Alle Infos (inkl. der Benutzer):
    - auf dem Silbertablett
  - ~~atime~~

Infos: Webseiten

- www.forensicswiki.org
- www.forinsect.de/forensics/forensics-tools.html
- www.sleuthkit.org, wiki.sleuthkit.org
- www.porcupine.org/forensics

  (TCT, Wietse Venema)

Infos: Lesestoff

- www.dfrws.org (Forensik-Konferenz)
- forensics@securityfocus.com
  (evtl. incidents+log-analysis)

- „Computer-Forensik“, dpunkt
- *der* Standard „Forensik Discovery“ per Download:
  www.porcupine.org/forensics/forensic-discovery/
- vielversprechend: 2008 (www.lob.de)

Danke für die Aufmerksamkeit! Fragen?

Dirk Wetter @ Dr. Wetter IT-Consulting
mail@drwetter.de

Sicherheitsanalysen, Digitale Forensik

Secure Linux Administration Conference 2, Berlin, 6.-7.12.2007