Recovery from a real rootkit attack

zeus.fh-brandenburg.de

Technisches Dokument, Nutzernamen geändert (trude, anton)

Dipl.-Inform. I. Boersch

[http://ots.fh-brandenburg.de/scripte ...]

- Eskalation am Freitag, 19.4.2002
- Spurensuche und Rekonstruktion des Angriffs
- Rekonstruktion des Systems
- Analyse
- Vorsorge
- Nützliche Dokumente
- Zusammenfassung: Recommended First Steps after a Rootkit Attack

Eskalation - Freitag 19.4.2002

10:00 Studenten: ls im ftp funktioniert nicht

10:10 Prüfung ls funktioniert auch nicht in einer Shell
ls: -> fehlende permissions to execute
su ebenfalls

10:20 ssh root@zeus klappt:
wichtige Systembefehle in /usr/bin sind nur für root executable

->EINBRUCH -> Eskalation

10:20 Information RZ, DI

10:25 zeus in single-user-Modus fahren
Booten
(war ein Fehler, da Spuren in /tmp und /dev/ und laufende Prozesse beseitigt werden)

Spurensuche

Dateien mit auffälligen Rechten in /usr/bin haben alle Änderungsdatum 19.4. 5:58 Uhr
in /usr/bin:

```
-rwx------   1 root     other      10740 Apr 19 05:58 du
-rwx------   1 root     other      10740 Apr 19 05:58 find
-rwx------   1 root     other      15380 Apr 19 05:58 ls
-r-s------   1 root     other      16364 Apr 19 05:58 m68k
-r-x------   1 root     other      41708 Apr 19 05:58 mc68000
-r-x------   1 root     other       7116 Apr 19 05:58 mc68010
-r-s------   1 root     other      35708 Apr 19 05:58 mc68020
-r-x------   1 root     other      17076 Apr 19 05:58 mc68030
-r-x--l---   1 root     other      31564 Apr 19 05:58 mc68040
-rwx------   1 root     other      10760 Apr 19 05:58 netstat
-rwx------   1 root     other      10040 Apr 19 05:58 passwd
-rwx------   1 root     other      11208 Apr 19 05:58 ps
-rwxr-xr-x   1 root     other     558868 Apr 19 05:58 sshd2
-rwx------   1 root     other      10040 Apr 19 05:58 su
-r-s--l---   1 root     other      15760 Apr 19 05:58 sun2
-r-s------   1 root     other      18780 Apr 19 05:58 sun3
-r-x------   1 root     other       7720 Apr 19 05:58 sun3x
-r-s------   1 root     other      47420 Apr 19 05:58 u370
-r-s------   1 root     other      11192 Apr 19 05:58 w
-rwx------   1 root     other     136288 Apr 19 05:58 wget
```

last

```
kirchnem  xdmremote    fhbxt1:0         Fri Apr 19 07:39 - 07:44  (00:05)
kirchnem  xdmremote                     Fri Apr 19 07:39 - 07:39  (00:00)
anton     ftp          pD9014226.dip.t- Fri Apr 19 07:23 - 07:44  (00:21)
anton     ftp          pD9014226.dip.t- Fri Apr 19 07:02 - 07:23  (00:21)
anton     ftp          pD9014226.dip.t- Fri Apr 19 06:40 - 07:02  (00:21)
anton     ftp          pD9014226.dip.t- Fri Apr 19 06:19 - 06:40  (00:21)
anton     ftp          pD9014226.dip.t- Fri Apr 19 05:58 - 06:19  (00:21)
trude    pts/7         silver.snut.ac.k Fri Apr 19 05:52 - 06:11  (00:18)
anton     ftp          pD9014226.dip.t- Fri Apr 19 05:36 - 05:58  (00:21)
anton     ftp          pD9014226.dip.t- Fri Apr 19 05:17 - 05:29  (00:12)
anton     ftp          pD9014226.dip.t- Fri Apr 19 05:15 - 05:17  (00:02)
anton     ftp          pD901422D.dip.t- Fri Apr 19 05:05 - 05:15  (00:09)
```

Korrelation mit Uhrzeit:

- Nutzer trude mit interaktiver Session (05:52 – 06:11)
- Nutzer anton mit ftp-Session (Beginn exakt 05:58 – 06:19)

Definition t0 = 19.Apr 05:58

Kontrolle

(0 heisst "keine Auffälligkteien")

0 Kontrolle hosts.equiv
0 alle .rhosts nach Datum
0 alle .forward nach Datum
0 sulog
0 pacct
0 messages

1 syslog->Probleme des sshd-zugeordneten pseudozufallszahlendamons prngd (fehlendes ls) begannen exact zu t0

1 setuid-Programme: mcxxx-Dateien in /usr/bin/sind setuid unnormal fuer crosscompiler, auch verdächtig wegen datum = t0

1 cronlog zu gross, nicht auswertbar -> Rollieren

Suche nach ebenfalls geänderten Dateien mit diesem Datum zeigt größeres Ausmaß

```
find / -mtime -2 -ls | grep .....
455225    1 drwxr-xr-x  4 root     sys          512 Apr 19 05:58 /usr/platform/sun4d
739880    1 drwx------  2 root     other        512 Apr 19 05:58 /usr/platform/sun4d/lib
739881    1 -rwx------  1 root     other        525 Apr 19 05:58 /usr/platform/sun4d/lib/ssh_host_key
739882    1 -rwx------  1 root     other        329 Apr 19 05:58 /usr/platform/sun4d/lib/ssh_host_key.pub
739883    1 -rwx------  1 root     other        512 Apr 19 05:58 /usr/platform/sun4d/lib/ssh_random_seed
739884    1 -rw-------  1 root     other        408 Apr 19 05:58 /usr/platform/sun4d/lib/sshd_config
243840    7 drwxrwxr-x  3 root     bin         7168 Apr 19 05:58 /usr/bin
243893   11 -rwx------  1 root     other      10740 Apr 19 05:58 /usr/bin/du
243908   11 -rwx------  1 root     other      10740 Apr 19 05:58 /usr/bin/find
244194   16 -rwx------  1 root     other      15380 Apr 19 05:58 /usr/bin/ls
244103   11 -rwx------  1 root     other      10760 Apr 19 05:58 /usr/bin/netstat
244195   10 -rwx------  1 root     other      10040 Apr 19 05:58 /usr/bin/passwd
244196   11 -rwx------  1 root     other      11208 Apr 19 05:58 /usr/bin/ps
243858   10 -rwx------  1 root     other      10040 Apr 19 05:58 /usr/bin/su
243971   16 -r-s------  1 root     other      16364 Apr 19 05:58 /usr/bin/m68k
244188   41 -r-x------  1 root     other      41708 Apr 19 05:58 /usr/bin/mc68000
244185    7 -r-x------  1 root     other       7116 Apr 19 05:58 /usr/bin/mc68010
244192   35 -r-s------  1 root     other      35708 Apr 19 05:58 /usr/bin/mc68020
244187   17 -r-x------  1 root     other      17076 Apr 19 05:58 /usr/bin/mc68030
244189   31 -r-x--s---  1 root     other      31564 Apr 19 05:58 /usr/bin/mc68040
244186   16 -r-s--s---  1 root     other      15760 Apr 19 05:58 /usr/bin/sun2
244145   19 -r-s------  1 root     other      18780 Apr 19 05:58 /usr/bin/sun3
244190    8 -r-x------  1 root     other       7720 Apr 19 05:58 /usr/bin/sun3x
244191   47 -r-s------  1 root     other      47420 Apr 19 05:58 /usr/bin/u370
244197   11 -r-s------  1 root     other      11192 Apr 19 05:58 /usr/bin/w
244193  560 -rwxr-xr-x  1 root     other     558868 Apr 19 05:58 /usr/bin/sshd2
244198  144 -rwx------  1 root     other     136288 Apr 19 05:58 /usr/bin/wget
349504    5 drwxrwxr-x 32 root     bin          4608 Apr 19 05:58 /usr/lib
617728    1 drwxr-xr-x  2 root     sys           512 Apr 19 05:58 /usr/lib/nfs
885994    1 drwxr-xr-x  3 bin      bin           512 Apr 19 05:58 /usr/lib/vold
349552   21 -rwx------  1 root     other      21424 Apr 19 05:58 /usr/lib/lpset
593347    5 drwxrwxr-x  2 root     bin          4608 Apr 19 05:58 /usr/openwin/bin
764032    5 drwxrwxr-x  6 root     bin          4608 Apr 19 05:58 /usr/sbin
764280   10 -rwx------  1 root     other      10040 Apr 19 05:58 /usr/sbin/ping
764306    0 -rw-------  1 root     other          0 Apr 19 05:58 /usr/sbin/in.fingerd
373991    2 drwxrwxr-x  3 root     bin          2048 Apr 19 05:58 /usr/ucb
374066   11 -rwx------  1 root     other      11208 Apr 19 05:58 /usr/ucb/ps
731665    1 drwx------  2 root     other         512 Apr 19 05:58 /usr/ucb/bin
731666   23 -rws------  1 root     other      23540 Apr 19 05:58 /usr/ucb/bin/ps
983488    4 drwxrwxr-x 28 root     sys          3584 Apr 19 05:58 /etc
56898    1 drwxrwxr-x  2 root     sys          1024 Apr 19 05:58 /etc/init.d
57330    1 -rw-------  1 root     other          18 Apr 19 05:58 /etc/init.d/network
983552    1 -rw-rw-r--  1 root     sys           920 Apr 19 05:58 /etc/inittab
```

tar der der gefundenen Dateien und Verzeichnisse

-> Überraschung: tar sichert Verzeichnisse, die find nicht angezeigt hat

-> rootkit (Reste) unter /usr/lib/vold/nsdap gefunden

-> Systembefehle sind komprommitiert
(unser 2. Fehler, Spurensicherung nur mit unkomprommiterten Befehlen durchführen)

12:00 - physische Trennung vom Netz
(sollte bei Einbruchserkennung erste Maßnahme sein)

- Booten von CD
- Probleme mit dem Datum da Zeitzone nicht sofort eingestellt wird
- mounten der root-platte
- aufspielen /cd/usr/bin nach /newbin; PATH setzen

Untersuchen rootkit /usr/lib/vold/nsdap

readme:

```
              #
    #
   #   #
    # # #       RootKit f³r SunOS
 #   #   #      (C) Adolf Hitler / NSDAP
  # # #
   #   #          English version.. for you scriptkids.
      #
     #
```

988113361

Dateien des rootkits

```
   cleaner $1  - löscht zeilen aus fast allen Dateien in /var/adm
               - bsp :  http://www.chinabyte.com/20020115/214049_6.shtml

   basepatch   - spielt eine os-dependend patch SUNWcsu ein
               Patch-ID#     106160-02
               Keywords:     security telnet login NULL HZ TZ
               Synopsis:     SunOS 5.5.1: /usr/bin/login patch
               Date:         Dec/13/2001) – fehlender gefährlich mit sadmind

   patcher     - sichert bestehende Versionen von ps, su, ping, login
               - spielt aktuellen Recommended_Patches ein,
               - sichern der neuen Versionen von ps, su, ping ,login
               - wiederherstellen der alten Versionen dieser Files

   sniffload   - installiert sniffer als /usr/lib/lpstart

   defines     - definiert Backup-Namen für original-Kommandos, z.B. mc68000 == ls
               (scheint zu stimmen in /usr/bin)

->mail: smith@mbox.bol.bg
- es fehlen files, z.B. wer benutzt "defines", setup-script!
```

16:30 Ausschalten
Feierabend 17:00, Rechner bleibt vom Netz

Abends (4 Stunden Suche+Analyse rootkit im WWW)
Google-Recherche -> Autor vermutlich Tragedy-Dor
http://openbsd.org.br/ouah/programmes.htm sehr ähnlicher trojaner vom gleichen autor unter rk18-1.tar.gz von 8/2000

Samstag 20.4.2002

Untersuchen sshd2-trojaner:

- Files: /etc/network,/etc/initab, usr/plattform/sun4d/lib->binary, Konfiguration und Keys für SSHD2
- neue zeile in der inittab startet sshd2-trojaner in jedem runlevel
- config setzt port auf 38479 -> damit kein Konflikt mit bestehendem sshd

0 ~anton
0 dfstab

adhoc-Sicherung: tar-file mit allen 5:58-Dateiene nach bacchus

14:45 Booten von CD
mounten: mount -F ufs /dev/dsk/c0t0d0so /tmp/mount/root
-> fsck: fsck /dev/rdsk/c0t0d0s0 -->ok

cd /tmp/mount/root; du -s .-> 1.5GB (2GB komplett) zu sichern
/local 3.4 GB
/home9/user/studenten 17GB , du -s . -> 9GB belegt
mount -F ufs /def/dsk/c0t4sod6 /tmp/mount/studenten

Komplettes Filesystem inclusive gelöschter Files sichern

```
15:10 Versuch dd in File
     dd if=/dev/dsk/c0t0d0s0 of=/tmp/mount/studenten/c0t0d0s0 bs=2k
     man: mount loop mgl unter solaris?
     22MB/10 sek ->2GB = 900 sek
     ls enthält Verweis auf trojener-configuration /etc/dhcp/dhcp.conf, aber file exisitert nicht
          (siehe gleicherangriff_john_kemp/msg00225.html)
     2.147481600 Bytes dd-Abzug der Fesplatte /tmp/studenten/c0t0d0s0
     mount -F ??
15:35     Wie mountet man ein fs-dump unter Solaris 2.5.1?
16:10 Erkenntnis: nloopback device erst ab solaris 8 (oder vorher fbk-Driver)
```

Komplettes Filesystem sichern:

```
16:15 ufsdump /tmp/mount/studenten/c0t0d0s0.ufsdump /dev/rdsk/c0t0d0s0
16:30 Suche: rootkit in studentenverzeichnis: find . -name nsdap* -print -> 0
16:40 extract funktioniert?
     vom ufsdump: ufsrestore xvf ufsdumpfilename /usr/bin/ls
          -> Frage nach volume: 1
          -> im aktuellen-Verzeichnis wird /usr/bin/ls angelegt ok
```

Sichern wichtiger Files auf einen W98-Laptop

```
16:46 /var/log liegt auf metadevice, ist im zustand booten von cd nicht mountbar
     booten von platte in singleusermodus, aktivieren der metadevices
17:10 mounten cdrom mit recommended patches
     /usr/bin/mount -F hsfs /dev/dsk/c0t6d0s0 /cdrom/ansys54_cd1

17:20 ftp-Server auf laptop installiert
     mount -a -> geht nicht ohne zeus250, Anschluß ans Netz
     sichern /var/log

17:45 Verkabelung das zeus+laptop im netz sind
     ./s69inetstart, Starten IP-Dienste

18:00 ftp aller logs zum laptop
```

Liste der Files

```
C0T0D0S0     2.147.475.456  20.04.02  17:21 c0t0d0s0            // dd-Abzug von /
C0T0D0~1 UFS 1.639.022.592  20.04.02  17:38 c0t0d0s0.ufsdump    // ufsdump der /
ANTON    TAR    25.271.296  20.04.02  17:41 anton.tar           // ~anton
VAR-LOG  TAR    35.568.128  20.04.02  17:43 var-log.tar         // /var/log
VAR-ADM  TAR   385.658.880  20.04.02  18:06 var-adm.tar         // /var/adm
NSDAP    TAR        76.800  20.04.02  18:08 nsdap.tar           // /usr/lib/vold/nsdap
USR-BIN  TAR    25.028.608  20.04.02  18:09 usr-bin.tar         // /usr/bin
558~1    TXT         3.548  20.04.02  18:27 5.58.txt            // alle Files mit mtime 19.4.2002
5:58 Uhr
FILENA~1 TXT           584  20.04.02  18:27 filenamen5.58.txt   // ditto nur Namen
FORWARD  TXT         6.144  20.04.02  18:27 forward.txt         // ls auf .forward
LAST     TXT     9.890.089  20.04.02  18:27 last.txt            // Ausgabe last
LAST2D~1 TXT        81.431  20.04.02  18:27 last2days-fake.txt  // angelegt ls aller Fehler mit
mtime der letzten 2 Tage mit fake-ls
LAST2D~2 TXT        22.431  20.04.02  18:27 last2days.txt       // angelegt mit cd-ls am 20.4.2002
-mtime -4
RHOSTS   TXT           877  20.04.02  18:27 rhosts.txt          // ls aller .rhosts
SUID20~1 TXT         9.230  20.04.02  18:27 suid.20020227.txt   // ls aller suid am 27.2.2002
SUID20~2 TXT         5.384  20.04.02  18:27 suid20020419.txt    // ls aller suid am 19.4.2002
u.v.a
```

19:30 Uhr

Test ist /usr/lib/lpset ein sniffer?

strings lpset -> offensichtlich ja, mitschneiden smtp, telnet, rsh/rlogin, ftp:

```
     filtering out smtp connections.
     filtering out telnet connections.
     filtering out rsh/rlogin connections.
     filtering out ftp connections.
     Usage: %s [-d x] [-s] [-f] [-l] [-t] [-i interface] [-o file]
     -d int    set new data limit (128 default)
     -s        filter out smtp connections
     -f        filter out ftp connections
     -l        filter out rlogin/rsh connections
     -t        filter out telnet connections
     -o <file> output to <file>

     -> output file optional -> wo ist das standard-ausgabefile?! ->stdout
      (siehe strings ...)
     - lpstart (snifferstart) exisitiert nicht
     - suche im fs-image nach lpset (auf laptop mit bview) 0
     0x5f22A30A Lage des rootkits im image (untersuchen mit bview)
```

20:45 Suche nach Kette lpset nicht erfolgreich (im image als auch auf der Platte)
Suche nach setup-Script im Image, (z.B. "heil" nach pacct), es ist zwar Platz von gelöschten Dateien zwischen den files des rootkits, leider hat die temporäre Ausgabe von last diesen Bereich überschrieben

21:30 trude-root-telnet mittels acctcom+syslog gefunden

Rekonstruktion des Angriffs (syslog, process-accounting)

5:52
Nutzer trude loggt sich vom Knoten silver.snut.ac.kr ein
(-> quota-cat-mail-Sequenz == /etc/profile)
kontrolliert auf installierte Backdoors und sniffer (passwd, lpxxx ...)
holt sich ein file mittels wget, auspacken mit tar, ein wenig umschauen

5:55 – 06:01
lokales telnet -> root (mit root-Passwort oder login-vuln.)
holt sich ein file mit rcp
auspacken mit tar
starten des rootkits-setups hitler (Laufzeit 26 Sekunden)

- startet u.a. sshd-trojaner
- verteilen von files im system
- fehlgeschlagener Versuch login-patch zu installieren (Dauer)
- stoppen, deaktivieren (inetd.conf) und löschen der Verzeichnisse von verschiedenen Dämonen
- Installation sniffer, Start schlägt fehl
- Sichern und ersetzen von Systembefehlen durch fake-versions
- Backdoors sshd, fingerd u.a

6:01 – 6:11
telnet zu einen nächsten Host (welchem?)

6:11 – nochmal kurz umgucken (uname),
ev. orientierungslos „Auf welchem Rechner bin ich eigentlich?“
- ausloggen

syslog (ohne Einträge für pop3d, smtpfwdd, smtpd, RCPT)

Apr 19 05:51:58 zeus in.telnetd[29249]: connect from silver.snut.ac.kr
Apr 19 05:55:45 zeus in.telnetd[29377]: connect from localhost
Apr 19 05:58:14 zeus in.ftpd[29626]: connect from pD9014226.dip.t-dialin.net
Apr 19 06:12:54 zeus smtpd[510]: smtp connection from UNKNOWN@bacchus(195.37.1.36) MAIL FROM: <>
RCPT TO: <kanthack@zeus.fh-brandenburg.de>, allowed by line 57 of /etc/smtpd_check_rules
Apr 19 06:19:34 zeus in.ftpd[710]: connect from pD9014226.dip.t-dialin.net

pacct (sortiert nach angangszeit, interaktive processe, +-1 sek):

```
                        START   END     REAL   CPU   MEAN
NAME     USER   TTYNAME         TIME    TIME   (SECS (SECS)  SIZE(K)

#in.ftpd root   ?       05:36:54        05:58:08     1274.88 Jan 19    1456.94        // anton
quota    trude  pts/7   05:52:24        05:52:24     0.14    0.02 1436.00   // login
cat      trude  pts/7   05:52:24        05:52:24     0.01    0.01 1432.00
mail     trude  pts/7   05:52:24        05:52:24     0.04    0.02 1108.00
uname    trude  pts/7   05:52:29        05:52:29     0.01    0.01 1712.00

ls       trude  pts/7   05:52:31        05:52:31     0.01    0.01 1672.00   // umschauen
w        trude  pts/7   05:52:48        05:52:48     0.07    0.07 964.57
ps       trude  pts/7   05:53:06        05:53:06     0.16    0.15 892.80
wget     trude  pts/7   05:53:45        05:53:45     0.14    0.03 845.33
ls       trude  pts/7   05:54:23        05:54:23     0.02    0.02 1272.00
wget     trude  pts/7   05:54:30        05:54:33     Mrz 48  0.07 1288.00   // holen URL 3sek,
kleines File
tar      trude  pts/7   05:54:35        05:54:35     0.25    0.07 834.29    // auspacken
msgfmt   trude  pts/7   05:54:39        05:54:39     0.04    0.01 1560.00
sh       trude  pts/7   05:54:39        05:54:39     0.05    0.02 764.00
passwd   trude  pts/7   05:54:39        05:54:39     0.09    0.04 732.00    // Kontrolle auf Trojaner
lpset    trude  pts/7   05:54:42        05:54:42     0.02    0.02 1168.00
id       trude  pts/7   05:54:46        05:54:46     0.03    0.01 2040.00   // wer bin ich
lpstat   trude  pts/7   05:54:53        05:54:54     Jan 20  0.79 909.77    // Kontrolle auf Trojaner
id       trude  pts/7   05:55:00        05:55:00     0.01    0.01 1296.00
tar      trude  pts/7   05:55:04        05:55:04     0.07    0.07 875.43
#rdist   trude  pts/7   05:55:15        05:55:15     0.08    0.03 1413.33
strings  trude  pts/7   05:55:25        05:55:25     0.03    0.02 1312.00
ls       trude  pts/7   05:55:31        05:55:31     0.02    0.01 1744.00

telnet   trude  pts/7   05:55:45        06:01:00     315.60  0.09 1374.22   // root login
in.telne root   ?       05:55:45        06:01:00     315.60  0.06 952.00
```

```
#sh      root   ?      05:55:45        06:01:00     315.44  0.10 740.80

quota    root   pts/11 05:55:50        05:55:50     0.01    0.01 808.00         // .profile
cat      root   pts/11 05:55:50        05:55:50     0.02    0.01 248.00
mail     root   pts/11 05:55:50        05:55:50     0.02    0.01 992.00
stty     root   pts/11 05:55:50        05:55:50     0.01    0.01 880.00

mkdir    root   pts/11 05:56:52        05:56:52     0.04    0.01 240.00
rcp      root   pts/11 05:57:01        05:57:16     15.68   0.12 1137.33        // holen od.
versenden eines Files 15 sek
pop32d   root   ?      05:57:05        05:58:20     75.59   0.03 1053.33
tar      root   pts/11 05:57:27        05:57:27     0.14    0.14 854.86         // auspacken,
kleines File
sh       root   pts/11 05:58:02        05:58:28     26.90   0.01 1208.00

hitler   root   pts/11 05:58:02        05:58:28     26.91   0.01 664.00         // start rootkit
cat      root   pts/11 05:58:03        05:58:03     0.01    0.01 1000.00
utime    root   pts/11 05:58:03        05:58:03     0.01    0.01 1256.00
heil     root   pts/11 05:58:03        05:58:03     0.01    0.01 1544.00
uname    root   pts/11 05:58:03        05:58:03     0.01    0.01 1264.00
uname    root   pts/11 05:58:03        05:58:03     0.01    0.01 1104.00
uname    root   pts/11 05:58:03        05:58:03     0.01    0.01 864.00
printf   root   pts/11 05:58:03        05:58:03     0.03    0.01 1464.00
cat      root   pts/11 05:58:03        05:58:03     0.18    0.01 680.00
cut      root   pts/11 05:58:03        05:58:03     0.22    0.20 816.00
cat      root   pts/11 05:58:03        05:58:03     0.03    0.01 272.00
grep     root   pts/11 05:58:03        05:58:03     0.03    0.02 712.00
cat      root   pts/11 05:58:03        05:58:03     0.02    0.01 688.00
grep     root   pts/11 05:58:03        05:58:03     0.02    0.02 928.00
cat      root   pts/11 05:58:03        05:58:03     0.02    0.02 504.00
grep     root   pts/11 05:58:03        05:58:03     0.03    0.01 1376.00
cat      root   pts/11 05:58:03        05:58:03     0.01    0.01 456.00
grep     root   pts/11 05:58:03        05:58:03     0.02    0.01 976.00
cat      root   pts/11 05:58:03        05:58:03     0.04    0.01 944.00
grep     root   pts/11 05:58:03        05:58:03     0.08    0.02 816.00
```

```
cat      root   pts/11 05:58:03       05:58:03     0.01    0.01 424.00
grep     root   pts/11 05:58:03       05:58:03     0.03    0.02 840.00
cat      root   pts/11 05:58:03       05:58:03     0.01    0.01 688.00
grep     root   pts/11 05:58:03       05:58:03     0.03    0.01 928.00
findkit  root   pts/11 05:58:03       05:58:11     Aug 53  0.39 929.23         // suche nach
installierten rootkits
heil     root   pts/11 05:58:03       05:58:29     26.89   0.16 869.50
cat      root   pts/11 05:58:04       05:58:04     0.01    0.01 688.00
grep     root   pts/11 05:58:04       05:58:04     0.02    0.01 1296.00
cat      root   pts/11 05:58:04       05:58:04     0.03    0.01 448.00
grep     root   pts/11 05:58:04       05:58:04     0.20    0.01 1376.00
cat      root   pts/11 05:58:04       05:58:04     0.02    0.02 612.00
grep     root   pts/11 05:58:04       05:58:04     0.03    0.01 1376.00
cat      root   pts/11 05:58:04       05:58:04     0.02    0.01 256.00
grep     root   pts/11 05:58:04       05:58:04     0.03    0.01 1208.00
cat      root   pts/11 05:58:04       05:58:04     0.04    0.01 416.00
grep     root   pts/11 05:58:04       05:58:04     0.04    0.01 1584.00
cat      root   pts/11 05:58:05       05:58:05     0.02    0.02 404.00
grep     root   pts/11 05:58:05       05:58:05     0.03    0.02 844.00
cat      root   pts/11 05:58:05       05:58:05     0.01    0.01 688.00
grep     root   pts/11 05:58:05       05:58:05     0.02    0.01 1344.00
cat      root   pts/11 05:58:08       05:58:08     0.02    0.01 488.00
grep     root   pts/11 05:58:08       05:58:08     0.03    0.02 948.00
cat      root   pts/11 05:58:09       05:58:09     0.01    0.01 696.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 752.00
cut      root   pts/11 05:58:09       05:58:09     0.01    0.01 448.00
wc       root   pts/11 05:58:09       05:58:09     0.06    0.02 936.00
cat      root   pts/11 05:58:09       05:58:09     0.03    0.02 616.00
grep     root   pts/11 05:58:09       05:58:09     0.03    0.01 712.00
cut      root   pts/11 05:58:09       05:58:09     0.03    0.02 432.00
wc       root   pts/11 05:58:09       05:58:09     0.04    0.02 892.00
cat      root   pts/11 05:58:09       05:58:09     0.02    0.02 604.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 392.00
cut      root   pts/11 05:58:09       05:58:09     0.02    0.02 528.00
wc       root   pts/11 05:58:09       05:58:09     0.04    0.02 676.00
```

```
cat      root   pts/11 05:58:09       05:58:09     0.02    0.01 264.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 572.00
cut      root   pts/11 05:58:09       05:58:09     0.02    0.02 672.00
wc       root   pts/11 05:58:09       05:58:09     0.04    0.02 1044.00
cat      root   pts/11 05:58:09       05:58:09     0.02    0.01 432.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 448.00
cut      root   pts/11 05:58:09       05:58:09     0.01    0.01 424.00
wc       root   pts/11 05:58:09       05:58:09     0.04    0.02 940.00
cat      root   pts/11 05:58:09       05:58:09     0.02    0.01 576.00
grep     root   pts/11 05:58:09       05:58:09     0.03    0.02 600.00
cut      root   pts/11 05:58:09       05:58:09     0.03    0.01 696.00
wc       root   pts/11 05:58:09       05:58:09     0.04    0.01 1232.00
cat      root   pts/11 05:58:09       05:58:09     0.02    0.02 632.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 600.00
cut      root   pts/11 05:58:09       05:58:09     0.02    0.01 952.00
wc       root   pts/11 05:58:09       05:58:09     0.07    0.01 1480.00
cat      root   pts/11 05:58:09       05:58:09     0.03    0.01 432.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 556.00
cut      root   pts/11 05:58:09       05:58:09     0.01    0.01 440.00
wc       root   pts/11 05:58:09       05:58:09     0.06    0.02 1080.00
cat      root   pts/11 05:58:09       05:58:09     0.04    0.02 608.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.01 264.00
cut      root   pts/11 05:58:09       05:58:09     0.01    0.01 704.00
wc       root   pts/11 05:58:09       05:58:09     0.10    0.01 1608.00
cat      root   pts/11 05:58:09       05:58:09     0.03    0.01 504.00
grep     root   pts/11 05:58:09       05:58:09     0.02    0.02 528.00
cut      root   pts/11 05:58:09       05:58:09     0.02    0.01 696.00
wc       root   pts/11 05:58:09       05:58:09     0.06    0.02 1100.00
cat      root   pts/11 05:58:09       05:58:09     0.12    0.01 696.00
grep     root   pts/11 05:58:09       05:58:09     0.15    0.01 712.00
cut      root   pts/11 05:58:09       05:58:09     0.14    0.02 624.00
wc       root   pts/11 05:58:09       05:58:09     0.17    0.01 920.00
cat      root   pts/11 05:58:10       05:58:10     0.03    0.01 576.00
grep     root   pts/11 05:58:10       05:58:10     0.02    0.02 632.00
cut      root   pts/11 05:58:10       05:58:10     0.01    0.01 704.00
```

```
wc      root   pts/11 05:58:10       05:58:10    0.11    0.01 1120.00
cat     root   pts/11 05:58:10       05:58:10    0.08    0.01 696.00
grep    root   pts/11 05:58:10       05:58:10    0.08    0.01 448.00
cut     root   pts/11 05:58:10       05:58:10    0.07    0.01 792.00
wc      root   pts/11 05:58:10       05:58:10    0.09    0.01 1360.00
cat     root   pts/11 05:58:10       05:58:10    0.02    0.01 792.00
grep    root   pts/11 05:58:10       05:58:10    0.02    0.02 672.00
cut     root   pts/11 05:58:10       05:58:10    0.01    0.01 504.00
wc      root   pts/11 05:58:10       05:58:10    0.03    0.02 688.00
cat     root   pts/11 05:58:10       05:58:10    0.01    0.01 696.00
grep    root   pts/11 05:58:10       05:58:10    0.02    0.02 548.00
cut     root   pts/11 05:58:10       05:58:10    0.02    0.01 704.00
wc      root   pts/11 05:58:10       05:58:10    0.03    0.01 1608.00
cat     root   pts/11 05:58:10       05:58:10    0.02    0.02 468.00
grep    root   pts/11 05:58:10       05:58:10    0.02    0.01 640.00
cut     root   pts/11 05:58:10       05:58:10    0.01    0.01 584.00
wc      root   pts/11 05:58:10       05:58:10    0.05    0.03 690.67
cat     root   pts/11 05:58:10       05:58:10    0.01    0.01 496.00
grep    root   pts/11 05:58:10       05:58:10    0.01    0.01 448.00
cut     root   pts/11 05:58:10       05:58:10    0.01    0.01 704.00
wc      root   pts/11 05:58:10       05:58:10    0.04    0.01 1352.00
cat     root   pts/11 05:58:10       05:58:10    0.03    0.01 688.00
grep    root   pts/11 05:58:10       05:58:10    0.01    0.01 768.00
cut     root   pts/11 05:58:10       05:58:10    0.01    0.01 584.00
wc      root   pts/11 05:58:10       05:58:10    0.09    0.02 936.00
find    root   pts/11 05:58:10       05:58:10    0.90    0.20 781.60
grep    root   pts/11 05:58:10       05:58:10    0.89    0.02 584.00
grep    root   pts/11 05:58:10       05:58:10    0.87    0.01 704.00
wc      root   pts/11 05:58:10       05:58:10    0.87    0.02 360.00
awk     root   pts/11 05:58:10       05:58:10    0.91    0.02 1060.00
mkdir   root   pts/11 05:58:11       05:58:11    0.08    0.01 1272.00
mkdir   root   pts/11 05:58:11       05:58:11    0.09    0.02 800.00
mkdir   root   pts/11 05:58:11       05:58:11    0.09    0.02 732.00
rpass   root   pts/11 05:58:11       05:58:11    0.01    0.01 840.00
pg      root   pts/11 05:58:11       05:58:11    0.02    0.02 988.00
```

```
cp       root   pts/11 05:58:11        05:58:11     0.04    0.02 1052.00
sh       root   pts/11 05:58:11        05:58:11     0.05    0.01 1048.00
#fix     root   pts/11 05:58:11        05:58:11     0.07    0.01 1168.00
printf   root   pts/11 05:58:12        05:58:12     0.01    0.01 1280.00
cat      root   pts/11 05:58:12        05:58:12     0.01    0.01 1240.00
cat      root   pts/11 05:58:12        05:58:12     0.01    0.01 1264.00
#crypt   root   pts/11 05:58:12        05:58:12     0.01    0.01 1200.00
cp       root   pts/11 05:58:12        05:58:12     0.01    0.01 840.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1280.00
rm       root   pts/11 05:58:12        05:58:12     0.03    0.01 1400.00
cp       root   pts/11 05:58:12        05:58:12     0.05    0.01 1280.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1280.00
cp       root   pts/11 05:58:12        05:58:12     0.06    0.01 1392.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1280.00
cp       root   pts/11 05:58:12        05:58:12     0.03    0.01 1328.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1112.00
cp       root   pts/11 05:58:12        05:58:12     0.04    0.02 912.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1280.00
cp       root   pts/11 05:58:12        05:58:12     0.04    0.02 800.00
rm       root   pts/11 05:58:12        05:58:12     0.03    0.01 1280.00
cp       root   pts/11 05:58:12        05:58:12     0.04    0.02 1040.00
rm       root   pts/11 05:58:12        05:58:12     0.03    0.01 1016.00
cp       root   pts/11 05:58:12        05:58:12     0.03    0.01 1280.00
rm       root   pts/11 05:58:12        05:58:12     0.02    0.01 1280.00
cp       root   pts/11 05:58:13        05:58:13     0.03    0.01 1280.00
rm       root   pts/11 05:58:13        05:58:13     0.02    0.01 840.00
cp       root   pts/11 05:58:13        05:58:13     0.03    0.02 1020.00
rm       root   pts/11 05:58:13        05:58:13     0.01    0.01 1280.00
cp       root   pts/11 05:58:13        05:58:13     0.03    0.01 1280.00
rm       root   pts/11 05:58:13        05:58:13     0.02    0.01 1280.00
cp       root   pts/11 05:58:13        05:58:13     0.06    0.01 1280.00
touch    root   pts/11 05:58:13        05:58:13     0.03    0.01 1240.00
uname    root   pts/11 05:58:13        05:58:13     0.01    0.01 1024.00
ls       root   pts/11 05:58:13        05:58:13     0.02    0.01 760.00
awk      root   pts/11 05:58:13        05:58:13     0.02    0.02 804.00
```

```
ls       root   pts/11 05:58:13       05:58:13     0.02    0.02 648.00
awk      root   pts/11 05:58:13       05:58:13     0.02    0.01 1160.00
expr     root   pts/11 05:58:13       05:58:13     0.01    0.01 1048.00
expr     root   pts/11 05:58:13       05:58:13     0.02    0.01 1488.00
expr     root   pts/11 05:58:13       05:58:13     0.01    0.01 832.00
printf   root   pts/11 05:58:13       05:58:13     0.01    0.01 1240.00
expr     root   pts/11 05:58:13       05:58:13     0.02    0.02 820.00
szl      root   pts/11 05:58:13       05:58:13     0.16    0.02 1084.00
cp       root   pts/11 05:58:13       05:58:13     0.03    0.01 1416.00
sh       root   pts/11 05:58:13       05:58:13     0.05    0.02 888.00
#fix     root   pts/11 05:58:13       05:58:13     0.06    0.01 1200.00
cp       root   pts/11 05:58:14       05:58:14     0.27    0.03 818.67
chmod    root   pts/11 05:58:14       05:58:14     0.01    0.01 1032.00
cat      root   pts/11 05:58:14       05:58:14     0.02    0.02 840.00
rm       root   pts/11 05:58:14       05:58:14     0.01    0.01 1240.00
cp       root   pts/11 05:58:14       05:58:14     0.40    0.02 1032.00
init     root   pts/11 05:58:14       05:58:14     0.05    0.01 1512.00
sshd2    root   pts/11 05:58:14       05:58:14     0.02    0.02 1048.00
uname    root   pts/11 05:58:14       05:58:14     0.01    0.01 1264.00
ls       root   pts/11 05:58:14       05:58:14     0.01    0.01 392.00
sshd2    root   ?      05:58:14       05:58:14     0.09    0.02 472.00
awk      root   pts/11 05:58:14       05:58:14     0.06    0.01 1704.00
sshd2    root   ?      05:58:14       05:58:14     0.02    0.02 444.00
ls       root   pts/11 05:58:14       05:58:14     0.02    0.01 320.00
awk      root   pts/11 05:58:14       05:58:14     0.04    0.01 1352.00
sshd2    root   ?      05:58:14       05:58:14     0.02    0.02 524.00
sz       root   pts/11 05:58:14       05:58:14     0.26    0.04 906.00
sshd2    root   ?      05:58:15       05:58:15     0.03    0.03 776.00
sshd2    root   ?      05:58:15       05:58:15     0.02    0.02 472.00
sshd2    root   ?      05:58:15       05:58:15     0.03    0.03 504.00
expr     root   pts/11 05:58:15       05:58:15     0.11    0.01 1280.00
expr     root   pts/11 05:58:15       05:58:15     0.01    0.01 1280.00
settime  root   pts/11 05:58:15       05:58:15     0.02    0.02 944.00
rm       root   pts/11 05:58:15       05:58:15     0.03    0.01 1280.00
cp       root   pts/11 05:58:15       05:58:15     0.12    0.02 936.00
```

```
sshd2    root   ?      05:58:15        05:58:15     0.04    0.02 804.00
sshd2    root   ?      05:58:15        05:58:15     0.03    0.03 562.67
sshd2    root   ?      05:58:15        05:58:15     0.19    0.02 560.00
uname    root   pts/11 05:58:15        05:58:15     0.11    0.01 1512.00
ls       root   pts/11 05:58:15        05:58:15     0.01    0.01 480.00
sshd2    root   ?      05:58:15        05:58:15     0.14    0.02 484.00
awk      root   pts/11 05:58:15        05:58:15     0.03    0.01 1360.00
ls       root   pts/11 05:58:15        05:58:15     0.02    0.02 392.00
awk      root   pts/11 05:58:15        05:58:15     0.04    0.02 1044.00
expr     root   pts/11 05:58:15        05:58:15     0.01    0.01 832.00
expr     root   pts/11 05:58:15        05:58:15     0.02    0.02 876.00
sz       root   pts/11 05:58:15        05:58:15     0.43    0.02 1092.00
settime  root   pts/11 05:58:15        05:58:15     0.01    0.01 1072.00
rm       root   pts/11 05:58:15        05:58:15     0.04    0.01 1280.00
cp       root   pts/11 05:58:15        05:58:15     0.04    0.01 1280.00
init     root   ?      05:58:15        05:58:15     0.21    0.01 296.00
uname    root   pts/11 05:58:16        05:58:16     0.02    0.01 864.00
mc68000  root   pts/11 05:58:16        05:58:16     0.01    0.01 760.00
mc68000  root   pts/11 05:58:16        05:58:16     0.24    0.02 1068.00
sh       root   pts/11 05:58:16        05:58:16     0.37    0.01 1280.00
mc68000  root   pts/11 05:58:16        05:58:16     0.02    0.02 952.00
ls       root   pts/11 05:58:16        05:58:16     0.60    0.01 424.00
awk      root   pts/11 05:58:16        05:58:16     0.60    0.01 1624.00
mc68000  root   pts/11 05:58:16        05:58:16     0.01    0.01 1272.00
mc68000  root   pts/11 05:58:16        05:58:16     0.03    0.03 834.67
sh       root   pts/11 05:58:16        05:58:16     0.05    0.01 1056.00
mc68000  root   pts/11 05:58:16        05:58:16     0.01    0.01 1224.00
ls       root   pts/11 05:58:16        05:58:16     0.09    0.02 560.00
awk      root   pts/11 05:58:16        05:58:16     0.09    0.01 1104.00
expr     root   pts/11 05:58:16        05:58:16     0.01    0.01 1152.00
expr     root   pts/11 05:58:16        05:58:16     0.01    0.01 1160.00
sz       root   pts/11 05:58:16        05:58:16     0.93    0.02 1092.00
settime  root   pts/11 05:58:17        05:58:17     0.01    0.01 840.00
rm       root   pts/11 05:58:17        05:58:17     0.03    0.02 908.00
cp       root   pts/11 05:58:17        05:58:17     0.03    0.01 960.00
```

```
uname    root   pts/11 05:58:17        05:58:17     0.01    0.01 1024.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1056.00
mc68000  root   pts/11 05:58:17        05:58:17     0.03    0.03 984.00
sh       root   pts/11 05:58:17        05:58:17     0.04    0.01 992.00
mc68000  root   pts/11 05:58:17        05:58:17     0.02    0.02 772.00
ls       root   pts/11 05:58:17        05:58:17     0.08    0.01 832.00
awk      root   pts/11 05:58:17        05:58:17     0.09    0.02 792.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1192.00
mc68000  root   pts/11 05:58:17        05:58:17     0.02    0.02 1068.00
sh       root   pts/11 05:58:17        05:58:17     0.03    0.01 1280.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1520.00
ls       root   pts/11 05:58:17        05:58:17     0.16    0.01 624.00
awk      root   pts/11 05:58:17        05:58:17     0.17    0.01 1240.00
expr     root   pts/11 05:58:17        05:58:17     0.01    0.01 1088.00
expr     root   pts/11 05:58:17        05:58:17     0.02    0.02 796.00
sz       root   pts/11 05:58:17        05:58:17     0.35    0.01 1352.00
settime  root   pts/11 05:58:17        05:58:17     0.01    0.01 840.00
rm       root   pts/11 05:58:17        05:58:17     0.04    0.02 700.00
cp       root   pts/11 05:58:17        05:58:17     0.03    0.01 1280.00
uname    root   pts/11 05:58:17        05:58:17     0.01    0.01 1000.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1064.00
mc68000  root   pts/11 05:58:17        05:58:17     0.02    0.02 1068.00
sh       root   pts/11 05:58:17        05:58:17     0.03    0.01 1408.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1216.00
ls       root   pts/11 05:58:17        05:58:17     0.09    0.02 856.00
awk      root   pts/11 05:58:17        05:58:17     0.10    0.02 516.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 960.00
mc68000  root   pts/11 05:58:17        05:58:17     0.02    0.02 1068.00
sh       root   pts/11 05:58:17        05:58:17     0.05    0.03 760.00
mc68000  root   pts/11 05:58:17        05:58:17     0.01    0.01 1224.00
ls       root   pts/11 05:58:17        05:58:17     0.08    0.01 616.00
awk      root   pts/11 05:58:17        05:58:17     0.08    0.01 1104.00
expr     root   pts/11 05:58:17        05:58:17     0.04    0.02 720.00
sz       root   pts/11 05:58:17        05:58:17     0.29    0.03 1005.33
#pop32d  boeingb       ?       05:58:17       05:58:17 0.67 0.03 1309.33
```

```
expr     root   pts/11 05:58:18        05:58:18     0.04    0.01 1280.00
settime  root   pts/11 05:58:18        05:58:18     0.02    0.01 1032.00
rm       root   pts/11 05:58:18        05:58:18     0.03    0.01 1616.00
cp       root   pts/11 05:58:18        05:58:18     0.03    0.01 1200.00
uname    root   pts/11 05:58:18        05:58:18     0.01    0.01 1224.00
mc68000  root   pts/11 05:58:18        05:58:18     0.03    0.02 1012.00
mc68000  root   pts/11 05:58:18        05:58:18     0.03    0.03 965.33
sh       root   pts/11 05:58:18        05:58:18     0.22    0.01 1272.00
mc68000  root   pts/11 05:58:18        05:58:18     0.01    0.01 1224.00
ls       root   pts/11 05:58:18        05:58:18     0.52    0.01 672.00
awk      root   pts/11 05:58:18        05:58:18     0.60    0.01 1240.00
mc68000  root   pts/11 05:58:18        05:58:18     0.01    0.01 1224.00
mc68000  root   pts/11 05:58:18        05:58:18     0.02    0.02 1068.00
sh       root   pts/11 05:58:18        05:58:18     0.03    0.01 1352.00
mc68000  root   pts/11 05:58:18        05:58:18     0.02    0.02 964.00
ls       root   pts/11 05:58:18        05:58:18     0.11    0.02 516.00
awk      root   pts/11 05:58:18        05:58:18     0.11    0.02 812.00
expr     root   pts/11 05:58:18        05:58:18     0.01    0.01 832.00
expr     root   pts/11 05:58:18        05:58:18     0.01    0.01 1280.00
sz       root   pts/11 05:58:18        05:58:18     0.97    0.04 900.00
settime  root   pts/11 05:58:19        05:58:19     0.01    0.01 1240.00
rm       root   pts/11 05:58:19        05:58:19     0.04    0.01 1416.00
cp       root   pts/11 05:58:19        05:58:19     0.03    0.01 1280.00
uname    root   pts/11 05:58:19        05:58:19     0.01    0.01 1264.00
mc68000  root   pts/11 05:58:19        05:58:19     0.01    0.01 1064.00
mc68000  root   pts/11 05:58:19        05:58:19     0.02    0.02 1068.00
sh       root   pts/11 05:58:19        05:58:19     0.11    0.02 792.00
mc68000  root   pts/11 05:58:19        05:58:19     0.02    0.02 1028.00
ls       root   pts/11 05:58:19        05:58:19     0.40    0.01 624.00
awk      root   pts/11 05:58:19        05:58:19     0.40    0.01 1232.00
mc68000  root   pts/11 05:58:19        05:58:19     0.01    0.01 1192.00
mc68000  root   pts/11 05:58:19        05:58:19     0.03    0.02 868.00
sh       root   pts/11 05:58:19        05:58:19     0.03    0.01 1592.00
mc68000  root   pts/11 05:58:19        05:58:19     0.02    0.02 892.00
ls       root   pts/11 05:58:19        05:58:19     0.11    0.01 624.00
```

```
awk      root   pts/11 05:58:19        05:58:19     0.11    0.01 1360.00
expr     root   pts/11 05:58:19        05:58:19     0.02    0.02 884.00
expr     root   pts/11 05:58:19        05:58:19     0.01    0.01 1280.00
sz       root   pts/11 05:58:19        05:58:19     0.95    0.02 892.00
settime  root   pts/11 05:58:20        05:58:20     0.01    0.01 1240.00
rm       root   pts/11 05:58:20        05:58:20     0.04    0.01 1272.00
cp       root   pts/11 05:58:20        05:58:20     0.03    0.01 840.00
cp       root   pts/11 05:58:20        05:58:20     0.01    0.01 1280.00
rm       root   pts/11 05:58:20        05:58:20     0.03    0.01 1040.00
cp       root   pts/11 05:58:20        05:58:20     0.04    0.01 1320.00
uname    root   pts/11 05:58:20        05:58:20     0.01    0.01 976.00
mc68000  root   pts/11 05:58:20        05:58:20     0.01    0.01 960.00
mc68000  root   pts/11 05:58:20        05:58:20     0.27    0.02 1216.00
sh       root   pts/11 05:58:20        05:58:20     0.30    0.01 1592.00
mc68000  root   pts/11 05:58:20        05:58:20     0.01    0.01 1224.00
ls       root   pts/11 05:58:20        05:58:20     0.34    0.02 628.00
awk      root   pts/11 05:58:20        05:58:20     0.35    0.02 752.00
mc68000  root   pts/11 05:58:20        05:58:20     0.01    0.01 1512.00
mc68000  root   pts/11 05:58:20        05:58:20     0.03    0.03 856.00
sh       root   pts/11 05:58:20        05:58:20     0.04    0.01 1272.00
mc68000  root   pts/11 05:58:20        05:58:20     0.01    0.01 1000.00
ls       root   pts/11 05:58:20        05:58:20     0.09    0.02 504.00
awk      root   pts/11 05:58:20        05:58:20     0.09    0.01 1360.00
expr     root   pts/11 05:58:20        05:58:20     0.01    0.01 1016.00
expr     root   pts/11 05:58:20        05:58:20     0.02    0.01 1720.00
sz       root   pts/11 05:58:20        05:58:20     0.68    0.01 1352.00
settime  root   pts/11 05:58:21        05:58:21     0.01    0.01 1240.00
rm       root   pts/11 05:58:21        05:58:21     0.04    0.02 976.00
cp       root   pts/11 05:58:21        05:58:21     0.02    0.01 1280.00
uname    root   pts/11 05:58:21        05:58:21     0.01    0.01 1264.00
mc68000  root   pts/11 05:58:21        05:58:21     0.01    0.01 760.00
mc68000  root   pts/11 05:58:21        05:58:21     0.22    0.03 922.67
sh       root   pts/11 05:58:21        05:58:21     0.41    0.01 1592.00
mc68000  root   pts/11 05:58:21        05:58:21     0.01    0.01 1224.00
ls       root   pts/11 05:58:21        05:58:21     0.48    0.01 248.00
```

```
awk      root   pts/11 05:58:21        05:58:21     0.51    0.01 832.00
mc68000  root   pts/11 05:58:21        05:58:21     0.02    0.02 800.00
mc68000  root   pts/11 05:58:21        05:58:21     0.03    0.03 837.33
sh       root   pts/11 05:58:21        05:58:21     0.04    0.01 760.00
mc68000  root   pts/11 05:58:21        05:58:21     0.01    0.01 1184.00
ls       root   pts/11 05:58:21        05:58:21     0.08    0.02 704.00
awk      root   pts/11 05:58:21        05:58:21     0.08    0.01 1624.00
expr     root   pts/11 05:58:21        05:58:21     0.02    0.02 948.00
expr     root   pts/11 05:58:21        05:58:21     0.01    0.01 1280.00
sz       root   pts/11 05:58:21        05:58:21     0.80    0.02 1036.00
settime  root   pts/11 05:58:21        05:58:21     0.01    0.01 1272.00
rm       root   pts/11 05:58:21        05:58:21     0.04    0.01 1016.00
cp       root   pts/11 05:58:21        05:58:21     0.02    0.01 1016.00
cp       root   pts/11 05:58:21        05:58:21     0.04    0.02 908.00
rm       root   pts/11 05:58:22        05:58:22     0.01    0.01 1416.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1280.00
cp       root   pts/11 05:58:22        05:58:22     0.09    0.01 1280.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1040.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1248.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.02 816.00
cp       root   pts/11 05:58:22        05:58:22     0.02    0.01 1280.00
cp       root   pts/11 05:58:22        05:58:22     0.02    0.01 1120.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1280.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1248.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1480.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1320.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1256.00
cp       root   pts/11 05:58:22        05:58:22     0.03    0.01 1408.00
cp       root   pts/11 05:58:22        05:58:22     0.02    0.01 1280.00
cp       root   pts/11 05:58:22        05:58:22     0.12    0.02 1172.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 872.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1128.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
```

```
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1040.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1280.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1264.00
chmod    root   pts/11 05:58:23        05:58:23     0.01    0.01 1008.00
chmod    root   pts/11 05:58:23        05:58:23     0.02    0.02 952.00
#chmod   root   pts/11 05:58:23        05:58:23     0.01    0.01 1272.00
chmod    root   pts/11 05:58:23        05:58:23     0.02    0.02 1020.00
#chmod   root   pts/11 05:58:23        05:58:23     0.01    0.01 1248.00
chmod    root   pts/11 05:58:23        05:58:23     0.17    0.04 926.00
#chmod   root   pts/11 05:58:23        05:58:23     0.03    0.01 1280.00
rpass    root   pts/11 05:58:23        05:58:23     0.01    0.01 1216.00
rm       root   pts/11 05:58:23        05:58:23     0.01    0.01 1280.00
touch    root   pts/11 05:58:23        05:58:23     0.04    0.01 1016.00
cat      root   pts/11 05:58:23        05:58:23     0.02    0.01 688.00
grep     root   pts/11 05:58:23        05:58:23     0.04    0.03 760.00
mv       root   pts/11 05:58:23        05:58:23     0.09    0.01 1288.00
rm       root   pts/11 05:58:24        05:58:24     0.06    0.01 1288.00
mc68020  root   pts/11 05:58:24        05:58:24     0.17    0.17 837.18
ps       root   pts/11 05:58:24        05:58:24     0.24    0.01 728.00
grep     root   pts/11 05:58:24        05:58:24     0.31    0.01 672.00
grep     root   pts/11 05:58:24        05:58:24     0.13    0.02 592.00
awk      root   pts/11 05:58:24        05:58:24     0.11    0.01 784.00
sh       root   pts/11 05:58:24        05:58:24     0.32    0.01 1360.00
cat      root   pts/11 05:58:24        05:58:24     0.01    0.01 488.00
grep     root   pts/11 05:58:24        05:58:24     0.02    0.01 848.00
mv       root   pts/11 05:58:24        05:58:24     0.09    0.01 1288.00
mc68020  root   pts/11 05:58:24        05:58:24     0.16    0.15 826.13
ps       root   pts/11 05:58:24        05:58:24     0.17    0.01 600.00
grep     root   pts/11 05:58:24        05:58:24     0.16    0.02 524.00
grep     root   pts/11 05:58:24        05:58:24     0.14    0.01 536.00
awk      root   pts/11 05:58:24        05:58:24     0.13    0.02 492.00
sh       root   pts/11 05:58:24        05:58:24     0.18    0.01 1160.00
rm       root   pts/11 05:58:24        05:58:24     0.01    0.01 1288.00
```

```
cat      root   pts/11 05:58:24        05:58:24     0.02    0.02 580.00
grep     root   pts/11 05:58:24        05:58:24     0.02    0.02 800.00
mv       root   pts/11 05:58:24        05:58:24     0.05    0.02 972.00
mc68020  root   pts/11 05:58:24        05:58:24     0.16    0.12 854.67
ps       root   pts/11 05:58:24        05:58:24     0.17    0.02 656.00
grep     root   pts/11 05:58:24        05:58:24     0.17    0.01 432.00
sh       root   pts/11 05:58:24        05:58:24     0.21    0.02 836.00
grep     root   pts/11 05:58:25        05:58:25     0.01    0.01 400.00
awk      root   pts/11 05:58:25        05:58:25     0.03    0.01 784.00
cat      root   pts/11 05:58:25        05:58:25     0.01    0.01 256.00
grep     root   pts/11 05:58:25        05:58:25     0.02    0.02 624.00
mv       root   pts/11 05:58:25        05:58:25     0.04    0.01 1288.00
mc68020  root   pts/11 05:58:25        05:58:25     0.17    0.16 855.50
ps       root   pts/11 05:58:25        05:58:25     0.23    0.03 642.67
grep     root   pts/11 05:58:25        05:58:25     0.22    0.01 440.00
grep     root   pts/11 05:58:25        05:58:25     0.28    0.01 440.00
awk      root   pts/11 05:58:25        05:58:25     0.39    0.01 752.00
sh       root   pts/11 05:58:25        05:58:25     0.43    0.02 744.00
rm       root   pts/11 05:58:25        05:58:25     0.08    0.01 1480.00
cat      root   pts/11 05:58:25        05:58:25     0.01    0.01 256.00
grep     root   pts/11 05:58:25        05:58:25     0.02    0.02 1148.00
mv       root   pts/11 05:58:25        05:58:25     0.05    0.01 1024.00
mc68020  root   pts/11 05:58:25        05:58:25     0.20    0.16 852.50
ps       root   pts/11 05:58:25        05:58:25     0.21    0.01 624.00
grep     root   pts/11 05:58:25        05:58:25     0.21    0.01 256.00
sh       root   pts/11 05:58:25        05:58:25     0.25    0.01 1360.00
grep     root   pts/11 05:58:26        05:58:26     0.01    0.01 256.00
awk      root   pts/11 05:58:26        05:58:26     0.02    0.02 848.00
cat      root   pts/11 05:58:26        05:58:26     0.01    0.01 688.00
grep     root   pts/11 05:58:26        05:58:26     0.02    0.01 1104.00
mv       root   pts/11 05:58:26        05:58:26     0.11    0.02 876.00
mc68020  root   pts/11 05:58:26        05:58:26     0.16    0.14 854.86
ps       root   pts/11 05:58:26        05:58:26     0.18    0.01 624.00
grep     root   pts/11 05:58:26        05:58:26     0.17    0.01 664.00
grep     root   pts/11 05:58:26        05:58:26     0.02    0.01 696.00
```

```
awk      root   pts/11 05:58:26        05:58:26     0.04    0.02 628.00
sh       root   pts/11 05:58:26        05:58:26     0.23    0.01 848.00
chmod    root   pts/11 05:58:26        05:58:26     0.03    0.01 1208.00
cat      root   pts/11 05:58:26        05:58:26     0.02    0.02 368.00
grep     root   pts/11 05:58:26        05:58:26     0.04    0.01 1064.00
mv       root   pts/11 05:58:26        05:58:26     0.08    0.01 1288.00
mc68020  root   pts/11 05:58:26        05:58:26     0.21    0.14 841.71
ps       root   pts/11 05:58:26        05:58:26     0.22    0.02 676.00
grep     root   pts/11 05:58:26        05:58:26     0.22    0.02 748.00
grep     root   pts/11 05:58:26        05:58:26     0.15    0.02 644.00
awk      root   pts/11 05:58:26        05:58:26     0.09    0.01 784.00
sh       root   pts/11 05:58:26        05:58:26     0.23    0.01 1360.00
mc68020  root   pts/11 05:58:26        05:58:26     0.17    0.17 851.29
ps       root   pts/11 05:58:26        05:58:26     0.19    0.01 624.00
grep     root   pts/11 05:58:26        05:58:26     0.17    0.01 464.00
grep     root   pts/11 05:58:26        05:58:26     0.16    0.01 264.00
awk      root   pts/11 05:58:26        05:58:26     0.15    0.02 724.00
sh       root   pts/11 05:58:26        05:58:26     0.19    0.01 848.00
mc68020  root   pts/11 05:58:27        05:58:27     0.16    0.13 885.54
ps       root   pts/11 05:58:27        05:58:27     0.18    0.04 664.00
grep     root   pts/11 05:58:27        05:58:27     0.17    0.01 304.00
grep     root   pts/11 05:58:27        05:58:27     0.16    0.02 512.00
awk      root   pts/11 05:58:27        05:58:27     0.14    0.01 784.00
sh       root   pts/11 05:58:27        05:58:27     0.20    0.01 848.00
mc68020  root   pts/11 05:58:27        05:58:27     0.16    0.16 822.50
ps       root   pts/11 05:58:27        05:58:27     0.17    0.02 496.00
grep     root   pts/11 05:58:27        05:58:27     0.18    0.02 748.00
grep     root   pts/11 05:58:27        05:58:27     0.01    0.01 712.00
awk      root   pts/11 05:58:27        05:58:27     0.01    0.01 592.00
sh       root   pts/11 05:58:27        05:58:27     0.25    0.02 784.00
mc68020  root   pts/11 05:58:27        05:58:27     0.16    0.15 821.87
ps       root   pts/11 05:58:27        05:58:27     0.17    0.01 256.00
grep     root   pts/11 05:58:27        05:58:27     0.17    0.01 328.00
grep     root   pts/11 05:58:27        05:58:27     0.05    0.01 696.00
awk      root   pts/11 05:58:27        05:58:27     0.03    0.01 784.00
```

```
sh       root   pts/11 05:58:27       05:58:27     0.19    0.02 800.00
rm       root   pts/11 05:58:27       05:58:27     0.01    0.01 1256.00
mc68020  root   pts/11 05:58:27       05:58:27     0.18    0.14 839.43
ps       root   pts/11 05:58:27       05:58:27     0.19    0.01 624.00
grep     root   pts/11 05:58:27       05:58:27     0.19    0.01 544.00
grep     root   pts/11 05:58:27       05:58:27     0.05    0.01 712.00
awk      root   pts/11 05:58:27       05:58:27     0.01    0.01 528.00
sh       root   pts/11 05:58:27       05:58:27     0.24    0.03 752.00
ps       root   pts/11 05:58:27       05:58:27     0.18    0.02 672.00
sh       root   pts/11 05:58:27       05:58:27     0.19    0.01 1496.00
mc68020  root   pts/11 05:58:28       05:58:28     0.17    0.13 847.38
grep     root   pts/11 05:58:28       05:58:28     0.17    0.02 680.00
awk      root   pts/11 05:58:28       05:58:28     0.16    0.01 576.00
mc68020  root   pts/11 05:58:28       05:58:28     0.15    0.14 823.43
ps       root   pts/11 05:58:28       05:58:28     0.17    0.02 508.00
grep     root   pts/11 05:58:28       05:58:28     0.17    0.02 468.00
awk      root   pts/11 05:58:28       05:58:28     0.15    0.01 488.00
sh       root   pts/11 05:58:28       05:58:28     0.17    0.02 1032.00
mc68020  root   pts/11 05:58:28       05:58:28     0.17    0.15 803.20
ps       root   pts/11 05:58:28       05:58:28     0.19    0.03 704.00
grep     root   pts/11 05:58:28       05:58:28     0.18    0.01 264.00
awk      root   pts/11 05:58:28       05:58:28     0.22    0.02 532.00
sh       root   pts/11 05:58:28       05:58:28     0.26    0.01 1112.00
mc68020  root   pts/11 05:58:28       05:58:28     0.17    0.15 802.67
ps       root   pts/11 05:58:28       05:58:28     0.18    0.01 264.00
grep     root   pts/11 05:58:28       05:58:28     0.17    0.01 264.00
awk      root   pts/11 05:58:28       05:58:28     0.16    0.02 696.00
sh       root   pts/11 05:58:28       05:58:28     0.18    0.01 848.00
rm       root   pts/11 05:58:28       05:58:28     0.01    0.01 1288.00
heil     root   pts/11 05:58:28       05:58:28     0.01    0.01 1600.00
uname    root   pts/11 05:58:28       05:58:28     0.02    0.02 668.00
basepatc root   pts/11 05:58:28       05:58:28     0.01    0.01 832.00    // nicht geklappt
mkdir    root   pts/11 05:58:28       05:58:28     0.02    0.02 724.00
cp       root   pts/11 05:58:28       05:58:28     0.08    0.01 1256.00
cp       root   pts/11 05:58:28       05:58:28     0.03    0.02 812.00
```

```
printf   root   pts/11 05:58:28        05:58:28     0.01    0.01 1008.00
basepatc root   pts/11 05:58:28        05:58:28     0.11    0.04 746.00
ifconfig root   pts/11 05:58:28        05:58:28     0.14    0.01 656.00
head     root   pts/11 05:58:28        05:58:28     0.09    0.03 682.67
grep     root   pts/11 05:58:28        05:58:28     0.09    0.01 952.00
grep     root   pts/11 05:58:28        05:58:28     0.09    0.01 704.00
awk      root   pts/11 05:58:28        05:58:28     0.15    0.02 708.00
heil     root   pts/11 05:58:29        05:58:29     0.01    0.01 256.00
cut      root   pts/11 05:58:29        05:58:29     0.01    0.01 1024.00
cp       root   pts/11 05:58:29        05:58:29     0.04    0.01 1280.00
chmod    root   pts/11 05:58:29        05:58:29     0.01    0.01 1008.00
rm       root   pts/11 05:58:29        05:58:29     0.02    0.02 1012.00
ifconfig root   pts/11 05:58:29        05:58:29     0.02    0.02 532.00
grep     root   pts/11 05:58:29        05:58:29     0.01    0.01 704.00
head     root   pts/11 05:58:29        05:58:29     0.01    0.01 424.00
grep     root   pts/11 05:58:29        05:58:29     0.01    0.01 600.00
awk      root   pts/11 05:58:29        05:58:29     0.08    0.01 1368.00
ifconfig root   pts/11 05:58:29        05:58:29     0.03    0.02 552.00
grep     root   pts/11 05:58:29        05:58:29     0.01    0.01 672.00
grep     root   pts/11 05:58:29        05:58:29     0.02    0.02 420.00
wc       root   pts/11 05:58:29        05:58:29     0.13    0.01 1272.00
uname    root   pts/11 05:58:29        05:58:29     0.02    0.02 832.00
dmesg    root   pts/11 05:58:29        05:58:29     0.34    0.28 931.71
grep     root   pts/11 05:58:29        05:58:29     0.21    0.01 672.00
head     root   pts/11 05:58:29        05:58:29     0.34    0.02 632.00
utime    root   pts/11 05:58:30        05:58:30     0.01    0.01 840.00
expr     root   pts/11 05:58:30        05:58:30     0.02    0.02 968.00
uname    root   pts/11 05:58:30        05:58:30     0.01    0.01 1240.00
uptime   root   pts/11 05:58:30        05:58:30     0.02    0.02 820.00
uname    root   pts/11 05:58:30        05:58:30     0.01    0.01 1264.00
hostname root   pts/11 05:58:30        05:58:30     0.03    0.02 1044.00
ifconfig root   pts/11 05:59:07        05:59:07     0.03    0.03 488.00
#telnet  root   pts/11 05:59:59        06:00:02     Mrz 45  0.02 1068.00
#telnet  root   pts/11 06:00:07        06:00:09     Feb 72  0.02 612.00
tail     root   pts/11 06:00:20        06:00:20     0.01    0.01 240.00
```

```
cat      root   pts/11 06:00:29        06:00:29     0.01    0.01 864.00
#rcp     root   pts/11 06:00:54        06:00:55     Jan 45  0.02 1068.00
telnet   trude  pts/7  06:01:18        06:11:07     589.84  0.14 1329.14        // another telnet
uname    trude  pts/7  06:11:12        06:11:12     0.01    0.01 1680.00        // orientierungslos

// ein alter dämon wird gekillt
rpc.rsta root   ?      08:28:07        05:57:50     250183.68    52.07     947.11
#statd   daemon ?      23:28:32        05:54:04     1232732.16   0.06 1114.67
```

rootkit: verwendetet Befehle und Häufigkeit

77 grep	3 ifconfig
46 cp	3 head
45 cat	3 #chmod
42 **mc68000**	2 utime
39 awk	2 **touch**
32 sh	2 **rpass**
31 rm	2 init
23 expr	2 **basepatc**
20 wc	2 #fix
20 ls	1 uptime
20 cut	1 szl
17 uname	1 pg
17 **chmod**	1 hostname
16 ps	1 **findkit**
16 mc68020	1 find
11 sshd2	1 dmesg
9 **sz**	1 **#crypt**
9 settime	
7 mv	
4 printf	
4 mkdir	
4 heil	

```
0 sulog: anton?
0 sulog trude
```

Kontrollen abgeleitet aus Quelle [8/2000 = altes ähnliches rootkit]

```
Spuren:
     DEL       ps spart sshd aus

     DEL       netstat spart ports aus: 13000,25000,6667,8000,9000

     DEL       0 Byte /usr/sbin/in.fingerd -> wurde gelöscht
               In 8/2000: öffnet shell über inetd auf port ingreslock , erzeugt dazu /tmp/bob

     DIENSTE   rpc.ttdbserverd, rpc.sadmind, rpc.cmsd, rpc.statd disabled:
               processkill, entfernen aus inetd.conf, Verzeichnisse und Dateien löschen

     YES       /usr/lib/lpset ist sniffer-binary, /usr/lib/lpstart ist sniffer-startscript?

Keine Spuren:
     NOEX      /etc/ttyhash? passwd des rootkits -> z.B im sshd, fingerd.in, login,su
     NOEX      /sbin/xlogin == originales login oder trojaner
     NOEX      /etc/rc2 und rc3 sshd-Eintrag, lpstart-Eintrag?
     NOEX      /usr/lib/ldlibnet.so und /usr/bin/netstat troj
     NOEX      sh im inetd.conf
     NOEX      Ex. ldlibps.so == originales ps-file oder vorheriger trojaner
     NOEX      Ex. ldlibnet.so == original netstat oder vorheriger trojaner
     NOEX      /dev/pts/... suchen nach snifferfile 0
     NOEX      root äuivalente accounts?
     NOEX      inetd.conf rje-eintrag?
     NOEX      dtspcd abschalten http://www.cert.org/advisories/CA-2002-01.html
```

Spurensicherung auf zeus beendet

Rekonstruktion

(Neuinstallation wäre nötig, dauert aber wegen Personalsituation im FBI zu lange)

Passwörter ändern:
- root

Login sperren
- trude/anton (passwd -l trude)

Files löschen /usr/bin/5:58
- /usr/platform/sun4d/lib/5:58
- /usr/lib/vold/nsdap
- /usr/lib/lpset
- /usr/openwin/bin wurde vermutlivh rpc.cmsd gelöscht nix geändert
- /usr/sbin/ping
- /usr/ucb/ps
- /usr/ucb/bin/ps
- /usr/ucb/bin-Verzeichnis gelöscht

Kontrolle /dev: Keine Files
- /etc/init.de/network (unsinnige Datei mit sshd-Eintrag)
- /etc/inittab korrigiert (letzte zeile entfernt)

23:30
- Kontrolle /usr/sbin/snoop für normalen nutzer, ->nicht möglich

Files:

cp -p /newbin/* /usr/bin // Copy CD-Tools rechterhaltend -p

Recommended PATCHES installieren

```
     auspacken, CLUSTER-README, SPECIAL-INSTRUCTIONS,
     vor dem patch:umask 022 d.h schreibit für user und gruppe wird ausgeblendet (standard
     rootumask 0077, keiner darf lesen)

0:05          .install_cluster (in tmp...)

0:50 patch beendet
          Logs kontrollieren auf fehlgeschlagene Patches
          Einzellogs: /var/sadm/patch/xxx-xxx/log
          Gesamtlog: /var/sadm/install_data/install_log

          Patch-Nacharbeiten:
          - /usr/lib/sendmail ist eigentlich smail,
            deshalb nach dem patch wieder hardlinks mailq, rsmtp, runq, sendmail auf smail

          /usr/lib/lpset löschen
          ok /usr/lib/nfs/rstatd
          ok /usr/sbin/in.fingerd
          ok /usr/openwin/bin/rpc.cmsd
          ok /usr/ucb/ps          // von wotan restauriert
          ok /usr/sbin/ping       // von wotan restauriert

          /new + /newbin /home/9/user/studenten bewegen und zugriff sichern
               -> nach /home9/user/studenten/new enthält alle Spurensicherungsfiles

01:15     Konfigurationen:

          DEAKTIVIERT in inetd.conf:    name, talk, finger, discard, KCMS Profile Server
          fs, ftp, telnetd
          AKTIVIERT in inetd.conf:      rpc.rstatd
          /etc/rc1.d mit Kxxxx -> Kill-Scripte
          /etc/rc2.d mit Sxxxx-> start-Scripte (Deaktivierung bei kleinem Anfangsbuchstaben)
          /etc/rc2.d/S72inetsvc: Änderung inetd -s -t      // -t logt ip+port in syslog
```

```
02:15     chkrootkit compiliert, keine Rootkits gefunden
          aktuelle suid-liste anlegen

02:45     find bricht mit cannot open :/ ab -> Lesefehler cdrom 3comvl -> umount

03:00     md5-Liste anlegen
          find / -type f -print|xargs  -t md5 2>/dev/null >md5-20020419.txt &

04:00     Neustart:Runlevel boot -r     (Neu erstellen der devices ...)
          smail von wotan über /usr/lib/smail (scheint durch patch ersetzt)

04:17     init 6
          netstat - Kontrolle unbekannte ports - jede Menge

User-Sniffer möglich?
          snoop/promisc-mode? 0

Kontrolle der laufenden Dienste ok
```

Sonntag   04:30   Feierabend

Analyse des Angriffs

Netzwerklogs im RZ-router vergleichen: ok
- ➔ poseidon, athene, bacchus
- ➔ z.B. athene: sniffer am switch, rootkit t0rn seit 2000

ssh_host_key.pub: Infos: keine Info

rootkit finden im W3 finden: nicht mehr gefunden

CERT, admin des silver.snut.ac.kr (SNUT = Seoul National University of Technology) verständigen: ok

Auszug aus /dev/prom/sn.l (athene)

```
-- TCP/IP LOG -- TM: Mon Mar 11 09:44:54 --
 PATH: zeus.fh-brandenburg.de(51959) => athene(telnet)
 STAT: Mon Mar 11 09:48:21, 335 pkts, 358 bytes [TH_FIN]
 DATA: (255)(253)^C(255)(251)^X(255)(251)^_(255)(251)
(255)(251)!(255)(251)"(255)(251)'(255)(253)^E(255)(251)#(255)(250)^_
     : }
     : =(255)(240)(255)(252)$(255)(250)^X
     : SUN-CMD(255)(240)(255)(250)#
     : kanthack:0.0(255)(240)(255)(250)'
     : DISPLAY^Akanthack:0.0(255)(240)(255)(253)^A(255)(252)^Akanthack
     : 7sieben
     : su
     : 1234qw
     : =(255)(240)passwd root
     : Qay1234
     : Qay1234
     : exit
     : su
     : Qay12234
     : su
     : Qay1234
     : cd 7etc
     : cd /etc
     : grep stamm passwd
     : vi passwd
     : (255)(250)^_
     : }
     : =(255)(240)^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[Bi#^[ZZ:w!
     : ZZsu stammler
     : exit
```

Vorsorge

Vorsorge - erledigt

COPS täglich ok
Chkrootkit täglich ok
md5-Vergleich aller Binaries mit CD oder _Netz
(Vergleich gegen www.sun.com...fingerprints.pl im Wesentlichen ok)
Suche nach snifferfile im image: not found
tripwire: ähnlich chk_rights, chk_files, chk_md5 nächtlich
cronlog rotieren ok
syslog maximal loggen ok
ftpd loggend starten (-l) ok
aktuelle sshd version ok

nessus-scan, offene ports jede Menge
Untersuchen Studentenproxys: lsof, truss
Gruppen geöffneter Ports:

Öffentliches Anbieten von Diensten privater Rechner
80 Anbieten von Webseiten aus dem Wohnheim
22 Anbieten von SSH-Zugang aus dem Wohnheim
3306 Anbieten von mysql-Zugang aus dem Wohnheim, ev. Sicherheitsproblem durch schlecht gewartete mysqld

Proxy für öffentliche Internetdienste zum Zugriff von privaten Adressen,
(imap, pop3 ...)

Proxy für öffentliche Webserver zum Zugriff von privaten Adressen
Problem Bandbreitenabrechnung, proxy.fh-brandenburg.de benutzen!

Proxy für Filesharing-Clients/Server z.B. SOCKSv5-Server für eDonkey genutzt

Sichern der Konfigurations- und Logfiles auf anderem Host (ok täglich)

Vorsorge – todo!

MITARBEITER EINSTELLEN!
Nicht benötigte Dienste abschalten (pop3, proxy der Studenten etc)
User security: local.stud aus dem Pfad entfernen
Warum meldet sich Nutzer anton nicht, obwohl sein login gesperrt ist?

Intrusion Detection – todo!

Snort im Netz u. local als IDS installieren
String aus shadow auf Platte suchen
Scannen aller lokalen Rechner auf installierte Sniffer (DNS, ping)

Nützliche Dokumente

- Nsdap-rootkit aus einem rootkit von 2000/Tragedy Door entwickelt, Analyse vom Honeynet-Projekt
  http://project.honeynet.org/scans/scan16/som/som13.txt

- Beschreibung eines Angriffs mit nsdap.tar.gz auf das Netz 128.223.0.0/16, John Kemp
  http://www.theorygroup.com/Archive/Unisog/2002/msg00225.html
- Steps for Recovering from a UNIX or NT System Compromise / Cert
  http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
- Decodieren des verschlüsselten Config-Files des Rootkits
  http://project.honeynet.org/scans/scan16/som/som17.html
  http://project.honeynet.org/scans/scan16/som/som34.html
- google: nsdap*tar*gz
  http://www.google.de/search?q=nsdap*tar*gz&hl=de&meta=
- Recognizing and Recovering from Rootkit, David O'Brien
  http://www.cs.wright.edu/people/faculty/pmateti/Courses/499/Fortification/obrien.html
- BIEW is Binary vIEW project – komfortabler und schneller Hex-Editor für Windows
  http://biew.sourceforge.net/
- Rootkit v. Tragedy Dor (8/2000), NSDAP-Rootkit
  http://ots.fh-brandenburg.de/rootkits/ (nur *.fh-brandenburg.de)

Zusammenfassung: Recommended First Steps after Rootkit Attack

Spurensicherung / Analyse

- Trennen vom Netz
- Mounten unkompromittierter Tools
- Sichern der raw-Filesysteme (dd, biew)
- Sichern und untersuchen von laufenden Prozessen (ps ,truss, strings, lsof)
- Sichern und Suchen von Dateien (find, strings, md5, tar)
- Sichern und untersuchen von logfiles (messages, syslog, debug, apachelogs, pacct ...)
- Sichern und untersuchen von Backdoors, Trojanern, Sniffern, Konfigurationsfiles
- Netz aktivieren: Sichern der Files auf andere Rechner
- Suche nach Quellen des Rootkits

Rekonstruktion/Neuinstallation

- Booten von CD ohne Netz, mounten der komprommitierten fs
- Ersetzen kompromittierter Files, Konfigurationen durch Originale
- Wiederherstellen von Diensten
- Einspielen aktueller Patches

Analyse

- Finden anderer betroffener Rechner, Logfiles der Aussenrouter
- Stringsuche im Dump des Filessystems

Vorsorge

- Logging auf Maximal-Level
- Intrusion Detection aktivieren (md5-compares, ...)
- Abschalten nicht benötigter Dienste und (Außen-)Verbindungen
- Deaktivieren unnötiger Logins
- Scannen von innnen (cops, tiger, iss, chkrootkit,...) und aussen (nessus, portscanner, saint ...)

Tip

Lagern Sie keine unersetzbaren Dokumente auf Netzwerk-Rechnern!

Kontakt

I. Boersch wiss. MA FBI+M FHB boersch@fh-brandenburg.de
T. Bluhm MA RZ FHB bluhm@fh-brandenburg.de