Totalschaden. Ein gehackter Server auf dem Seziertisch.
[CeBIT Forum Open Source 2013]
Peer Heinlein <p.heinlein@heinlein-support.de>

# Totalschaden.

# Ein gehackter Server auf dem Seziertisch.

Peer Heinlein <p.heinlein@heinlein-support.de>

# Dieser Vortrag basiert auf einer wahren Begebenheit

- Die nachfolgende Geschichte hat sich *fast* genau so abgespielt.
  - Einige Dinge/Erkenntnisse wurden zur besseren Erklärung und/oder zur besseren Dramaturgie in der Reihenfolge etwas vertauscht.
  - Manchmal stand erst Erkenntnis/Verdacht im Raum und dann wurde der Beweis gefunden.
  - Listen-Ausgaben i.d.R. immer auf wesentliche Zeilen zusammengekürzt

Peer Heinlein <p.heinlein@heinlein-support.de>

# Dieser Vortrag basiert auf einer wahren Begebenheit

- Kein Protokollauszug hier läßt irgendwelche Rückschlüsse auf Kunden oder Beteiligte zu.

- Ähnlichkeiten mit lebenden Systemen oder Personen sind rein zufällig, nicht beabsichtigt und kein Hinweis auf Identitäten.

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Ausgangslage:

Ein Webshop-Server bei Server4You.

Peer Heinlein <p.heinlein@heinlein-support.de>

# Freitag, 28. Dezember

- LAMP-Server, PLESK-System, Web-Shop-System
- Server wurde von Server4You gesperrt, nachdem ausgehende Angriffe von diesem Server festgestellt worden waren.
- Kunde: Keine Ahnung was vor sich geht.
  - Shop ist tot. Feiertagsgeschäft geht flöten.
- 28.12.: Anruf des Kunden bei unserer 24/7-Hotline
  - Wir nehmen Kontakt mit Server4You auf, da der Kunde uns nicht erklären konnte, was hier los ist
  - Kundenname war dem Support-Team seufzend wohlbekannt
  - Wir kümmern uns drum – Server wird durch Server4You entsperrt

Peer Heinlein <p.heinlein@heinlein-support.de>

# Erster Blick:
# Eine vor wenigen Tagen editierte Shadow-Datei.

```
root@hostxxx:/mnt/etc# ls -la passwd shadow
-rw-r--r-- 1 root root   1872 Dec 10 10:40 passwd
-rw-r----- 1 root shadow 1646 Dec 25 11:38 shadow
```

# Zweiter Blick:
# Wie sieht das denn von außen aus?

```
peer@booster:~> nmap 85.25.xxx.xxx

Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-28 13:03 CET
Nmap scan report for hostxxx.server4you.de (85.25.xxx.xxx)
Host is up (0.039s latency).
Not shown: 981 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
106/tcp  open     pop3pw
110/tcp  open     pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
993/tcp  open     imaps
995/tcp  open     pop3s
3306/tcp open     mysql
8080/tcp open     http-proxy
8443/tcp open     https-alt
9080/tcp open     glrpc
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Dritter Blick:
# Was haben wir denn im Plesk-Ordner?

```
hostxxx:~/parallels# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 904
drwxr-xr-x   6 root     root         4096 Dec 23 21:14 .
drwx------   7 root     root         4096 Dec 28 13:18 ..
-rwxrwxrwx   1 root     root         1191 Dec 23 21:14 1.pl
-rwxrwxrwx   1 root     root       147456 Dec 17 19:46 85.core
-rwxrwxrwx   1 root     root         2184 Dec 23 21:14 9C0.pl
drwxr-xr-x   2 root     root         4096 Dec 23 06:30 BILLING_11.0.9
drwxr-xr-x   2 root     root         4096 Dec 23 06:30 NGINX_1.3.0
drwxr-xr-x   4 root     root         4096 Dec 23 06:30 PSA_11.0.9
drwxr-xr-x   2 root     root         4096 Dec 23 06:30 SITEBUILDER_11.0.10
-rw-r--r--   1 root     root          867 Dec 23 06:30 apache.inf3
-rw-r--r--   1 root     root        32389 Dec 23 06:30 billing.inf3
-rwxrwxrwx   1 root     root         1183 Dec 23 21:14 floodJC.pl
-rwxrwxrwx   1 root     root         8979 Dec 14 13:26 gg
-rwxrwxrwx   1 root     root         8621 Dec 17 19:47 juno6
-rwxrwxrwx   1 root     root       147456 Dec 17 19:47 moo.core
-rw-r--r--   1 root     root         1537 Dec 23 06:30 mysql.inf3
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Dritter Blick:
# Was haben wir denn im Plesk-Ordner?

```
-rwxrwxrwx   1 root     root         8947 Dec 14 21:20 new
-rwxrwxrwx   1 root     root       147456 Dec 17 19:47 new.core
-rw-r--r--   1 root     root         3716 Dec 23 06:30 nginx.inf3
-rwxrwxrwx   1 root     root         1012 Dec 23 21:14 pinger.pl
-rw-r--r--   1 root     root       212411 Dec 23 06:30 plesk.inf3
-rw-r--r--   1 root     root        28499 Dec 23 06:30 pp-sitebuilder.inf3
-rw-r--r--   1 root     root        14116 Dec 23 06:30 ppsmbe.inf3
-rw-r--r--   1 root     root         1150 Dec 23 06:30 products.inf3
-rwxrwxrwx   1 root     root         8979 Dec 14 14:08 sahanqwhoiq
-rw-r--r--   1 root     root         5851 Dec 23 06:30 setemplates.inf3
-rw-r--r--   1 root     root        11376 Dec 23 06:30 sitebuilder.inf3
-rw-r--r--   1 root     root        10799 Dec 23 06:30 sso.inf3
-rwxrwxrwx   1 root     root         7830 Dec 14 21:20 udpillusion
-rwxrwxrwx   1 root     root         8666 Dec 14 14:08 ugg
-rwxrwxrwx   1 root     root         1076 Dec 23 21:14 vip.pl
-rwxrwxrwx   1 root     root         8979 Dec 14 21:20 vl
```

# Vierter Blick:
# Wer war denn hier wann auf dem System?

```
Dec 25 12:36:02 hostxxx sshd[29214]: Accepted password for
root from 82.61.xxx.xxx port 51992 ssh2
Dec 25 12:36:02 hostxxx sshd[29214]: pam_unix(sshd:session):
session opened for user root by (uid=0)
Dec 25 12:38:57 hostxxx passwd[29455]:
pam_unix(passwd:chauthtok): password changed for root
```

→ **Oha.**

# Tja. Was ist jetzt unser Fazit?

- Der Angreifer ist in Besitz des root-Passwortes gelangt
  - Der Angreifer konnte sich per SSH mit dem System verbinden und hat wohl Spaß gehabt.
- Erster Workaround: Zugriff per SSH durch iptables-Regel unterbunden
- Ansonsten sieht aber derzeit auf dem System alles ruhig aus.
  - Man müßte jetzt mehrere Stunden tiefergehend suchen.
  - Aber: Kunde wollte nur schnelle Freischaltung damit Shop wieder online ist mit wenig Aufwand, zunächst waren nur 2-3h genehmigt.
  - Echte Forensik hier mit dem zeitlichen Umfang nicht machbar/gewünscht
  - Also nach Rücksprache mit Kunden ab in die Sylvestertage.

Peer Heinlein <p.heinlein@heinlein-support.de>

# Teil 2.

Peer Heinlein <p.heinlein@heinlein-support.de>

# Die Story geht weiter…

- Wenige Tage später, 1. Januar um 2 Uhr nachts:
  E-Mail des Kunden im Ticketsystem
  - „Hallo, unser Server ist schon wieder geblockt oder sogar gesperrt. Ich hatte gedacht dass Sie noch am selben Abend den Server nach weiteren Schädlingen durchsuchen.“
- Also: Login auf dem Server in der Sylvesternacht um 4 Uhr (hicks!)
- SSH-Port von außen aber nach wie vor blockiert.
- Hmmm.

Peer Heinlein <p.heinlein@heinlein-support.de>

# netstat liefert keine Auffälligkeiten.

```
hostxxx:~# netstat -tulpen
Active Internet connections (only servers)
Proto Local Address           Foreign Address     State       User      PID/Program name
tcp   0.0.0.0:3306            0.0.0.0:*           LISTEN      104       1260/mysqld
tcp   127.0.0.1:10001         0.0.0.0:*           LISTEN      0         2871/sw-cp-serverd
tcp   0.0.0.0:465             0.0.0.0:*           LISTEN      0         1506/master
tcp   85.25.xxx.xxx:53          0.0.0.0:*         LISTEN      106       937/named
tcp   127.0.0.1:53            0.0.0.0:*           LISTEN      106       937/named
tcp   0.0.0.0:22              0.0.0.0:*           LISTEN      0         1745/sshd
tcp   127.0.0.1:3000          0.0.0.0:*           LISTEN      105       1952/drwebd.real
tcp   127.0.0.1:5432          0.0.0.0:*           LISTEN      108       1324/postgres
tcp   0.0.0.0:25              0.0.0.0:*           LISTEN      0         1506/master
tcp   127.0.0.1:953           0.0.0.0:*           LISTEN      106       937/named
tcp   127.0.0.1:12768         0.0.0.0:*           LISTEN      102       1114/psa-pc-remote
udp   85.25.xxx.xxx:53          0.0.0.0:*                     106       937/named
udp   127.0.0.1:53            0.0.0.0:*                     106       937/named
udp   85.25.xx.xx:137         0.0.0.0:*                     0         927/nmbd
udp   85.25.xxx.xxx:137         0.0.0.0:*                   0         927/nmbd
udp   0.0.0.0:137             0.0.0.0:*                     0         927/nmbd
udp   85.25.xx.xx:138         0.0.0.0:*                     0         927/nmbd
udp   85.25.xxx.xxx:138         0.0.0.0:*                   0         927/nmbd
Udp   0.0.0.0:138             0.0.0.0:*                     0         927/nmbd
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Sieht alles gut aus.

Aber...?

Peer Heinlein <p.heinlein@heinlein-support.de>

# Wo versteckt man was?
# Am besten direkt vor der Nase.

```
hostxxx:~# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 72
drwx------   9 root     root         4096 Jan  1 11:34 .
drwxr-xr-x  22 root     root         4096 Dec 30 06:48 ..
drwxr-xr-x   3 root     root         4096 Dec 30 09:23 ...
drwx------   2 root     root         4096 Jan  1 11:45 .aptitude
drwxr-xr-x   2 root     root         4096 Dec 23 06:34 .autoinstaller
-rw-------   1 root     root        14516 Jan  1 11:36 .bash_history
-rw-r--r--   1 root     root          402 Aug 10 22:10 .bashrc
-rw-------   1 root     root           54 Jan  1 11:00 .lesshst
drwx------   2 root     root         4096 Jan  1 11:36 .mc
-rw-r--r--   1 root     root          140 Nov 19  2007 .profile
drwx------   2 root     root         4096 Aug 11 06:28 .spamassassin
-rw-------   1 root     root         1240 Dec 20 23:21 .viminfo
drwxr-xr-x   5 root     root         4096 Jan  1 11:53 HPLS
drwxr-xr-x   6 root     root         4096 Jan  1 11:36 paralle
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Und siehe da:
# Die Geheimtür öffnet sich...

```
hostxxx:~# cd .../
hostxxx:~/...# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 32
drwxr-xr-x   3 root     root         4096 Dec 30 09:23 .
drwx------   9 root     root         4096 Jan  1 11:34 ..
drwx------   2 2112     2000         4096 Jan  1 10:52 .x
-rwxr-xr-x   1 root     root        17557 Jan 22  2011 mm
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Bezeichnende Funde in der Schatzkiste:

```
hostxxx:~/...# cd .x/
hostxxx:~/.../.x# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 7892
drwx------   2 2112     2000         4096 Jan  1 10:52 .
drwxr-xr-x   3 root     root         4096 Dec 30 09:23 ..
-rwx--x--x   1 2112     2000      1373863 Apr  8  2005 atac
-rw-r--r--   1 root     root      2520324 Jan  1 10:51 bios.txt
-rw-r--r--   1 root     root      2408983 Jan  1 10:52 mfu.txt
-rwx--x--x   1 2112     2000         1524 Jan  1 10:43 pass_file
-rwx--x--x   1 2112     2000       167964 Mar 16  2001 pico
-rwx--x--x   1 2112     2000       249980 Feb 13  2001 screen
-rwx--x--x   1 2112     2000       453972 Jul 12  2004 ss
-rwx--x--x   1 2112     2000       842736 Nov 24  2004 ssh-scan
-rwx--x--x   1 2112     2000          481 Feb  2  2011 x
```

# Nochmal zurück: Wo ist hier was offen?

```
hostxxx:~# netstat -tulpen
Active Internet connections (only servers)
Proto Local Address           Foreign Address     State       User     PID/Program name
tcp   0.0.0.0:3306            0.0.0.0:*           LISTEN      104      1260/mysqld
tcp   127.0.0.1:10001         0.0.0.0:*           LISTEN      0        2871/sw-cp-serverd
tcp   0.0.0.0:465             0.0.0.0:*           LISTEN      0        1506/master
tcp   85.25.xxx.xxx:53          0.0.0.0:*         LISTEN      106      937/named
tcp   127.0.0.1:53            0.0.0.0:*           LISTEN      106      937/named
tcp   0.0.0.0:22              0.0.0.0:*           LISTEN      0        1745/sshd
tcp   127.0.0.1:3000          0.0.0.0:*           LISTEN      105      1952/drwebd.real
tcp   127.0.0.1:5432          0.0.0.0:*           LISTEN      108      1324/postgres
tcp   0.0.0.0:25              0.0.0.0:*           LISTEN      0        1506/master
tcp   127.0.0.1:953           0.0.0.0:*           LISTEN      106      937/named
tcp   127.0.0.1:12768         0.0.0.0:*           LISTEN      102      1114/psa-pc-remote
udp   85.25.xxx.xxx:53          0.0.0.0:*                     106      937/named
udp   127.0.0.1:53            0.0.0.0:*                     106      937/named
udp   85.25.xxx.x:137         0.0.0.0:*                     0        927/nmbd
udp   85.25.xxx.xxx:137         0.0.0.0:*                   0        927/nmbd
udp   0.0.0.0:137             0.0.0.0:*                     0        927/nmbd
udp   85.25.x.xxx:138         0.0.0.0:*                     0        927/nmbd
udp   85.25.xxx.xxx:138         0.0.0.0:*                   0        927/nmbd
Udp   0.0.0.0:138             0.0.0.0:*                     0        927/nmbd
```

# Wechseln wir die Betrachtungsart

- Also: Nehmen wir ein anderes Tool: lsof statt netstat

```
hostxxx:~# lsof -i
COMMAND     PID         USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
[...]
3          1738         root    4u  IPv4 48649190      0t0  TCP hostxxx.server4you.de:112-
>hostxxxx-244-dynamic.xx-82-r.retail.telecomitalia.it:49283 (ESTABLISHED)
3          1984         root    3u  IPv4     7844      0t0  TCP *:112 (LISTEN)
[...]
```

- Port 112 war offen und in Benutzung.
- You are not alone...
- Oha.

# Und sonst noch?

→ Kiloweise interessante Prozesse...

```
hostxxx:~# lsof -i
[...]
ssh-scan  22238          root    6u  IPv4 51099726      0t0  TCP
hostxxx.server4you.de:37443->72.xx.79ae.static.somewhere.xyz:22 (ESTABLISHED)
ssh-scan  22316          root    6u  IPv4 51098992      0t0  TCP
hostxxx.server4you.de:37768->fb.xx.79ae.static.somewhere.xyz:22 (ESTABLISHED)
ssh-scan  22340          root    6u  IPv4 51099950      0t0  TCP
hostxxx.server4you.de:36435->3c.xx.79ae.static.somewhere.xyz:22 (ESTABLISHED)
ssh-scan  22351          root    6u  IPv4 51099126      0t0  TCP
hostxxx.server4you.de:46659->0.xx.79ae.static.somewhere.xyz:22 (ESTABLISHED)
ssh-scan  22372          root    6u  IPv4 51099446      0t0  TCP
hostxxx.server4you.de:35364->88.xx.79ae.static.somewhere.xyz:22 (ESTABLISHED)
```

→ Alles klar.

Peer Heinlein <p.heinlein@heinlein-support.de>

# Wo ist unser Prozeß "3" ?!?

```
hostxxx:~# ps ax
Warning: /boot/System.map-2.6.32-5-amd64 has an incorrect kernel version.
  PID TTY      STAT   TIME COMMAND
[...]
 1132 ?        S      0:00 /bin/sh /usr/bin/mysqld_safe
 1260 ?        S      1:57 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql
--user=mysql --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock
--port=3306
 1261 ?        S      0:00 logger -t mysqld -p daemon.error
 1324 ?        S      0:01 /usr/lib/postgresql/8.x/bin/postgres -D
/var/lib/postgresql/8.x/main -c config_file=/etc/postgresql/8.x/main/postgresql.conf
 1412 ?        S      0:10 postgres: writer process

 1745 ?        S      0:00 /usr/sbin/sshd
 1952 ?        S     19:14 drwebd.real
 2871 ?        S      0:39 /usr/sbin/sw-cp-serverd -f /etc/sw-cp-server/config
13848 ?        S      0:00 drwebd.real
16185 ?        S      0:00 /usr/sbin/apache2 -k start
17381 ?        S      0:00 /usr/bin/sw-engine-cgi -c /opt/psa/admin/conf/php.ini -d
auto_prepend_file=auth.php3 -u psaadm
29781 ?        S      0:00 sshd: root@pts/1
29805 pts/1    S      0:00 -bash
hostxxx:~#
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Rücken wir Prozeß "3" mit der PID 1984 auf den Leib

```
hostxxx:/usr# cd /proc/1984/
hostxxx:/proc/1984# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 0
-r--r--r--   1 root     root            0 Jan  1 12:21 cpuset
lrwxrwxrwx   1 root     root            0 Jan  1 11:54 cwd -> /
-r--------   1 root     root            0 Jan  1 11:36 environ
lrwxrwxrwx   1 root     root            0 Jan  1 11:38 exe -> /tmp/sh-A40PGA2AB35 (deleted)
dr-x------   2 root     root            0 Jan  1 11:47 fd
dr-x------   2 root     root            0 Jan  1 11:47 fdinfo
-r--------   1 root     root            0 Jan  1 12:21 io
-r--r--r--   1 root     root            0 Jan  1 12:21 pagemap
-r--r--r--   1 root     root            0 Jan  1 12:21 personality
lrwxrwxrwx   1 root     root            0 Jan  1 11:54 root -> /
-rw-r--r--   1 root     root            0 Jan  1 12:21 sched
-r--r--r--   1 root     root            0 Jan  1 12:21 wchan
hostxxx:/proc/1984#
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Und was läuft da auf Port 112?

```
booster:/home/peer/xxxxxx-Server # telnet 85.25.xxx.xxx 112
Trying 85.25.xxx.xxx...
Connected to 85.25.xxx.xxx.
Escape character is '^]'.
SSH-1.5-2.0.13

Protocol mismatch.
Connection closed by foreign host.
booster:/home/peer/xxxxxx-Server #
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Was passiert eigentlich, wenn man den Angreifer rauskickt?

```
hostxxx:~# lsof -i :112
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
3       1984 root    3u  IPv4   8903      0t0  TCP *:112 (LISTEN)
3       2142 root    4u  IPv4   8907      0t0  TCP
hostxxx.server4you.de:112->p5795xxxF.dip.t-dialin.net:40250 (ESTABLISHED)
hostxxx:~#
```

# Wer ist denn unser unerwünschter Gast?

- Eben noch in Italien, wenige Sekunden später aus Deutschland. Später auch Türkei und andere Länder...
  - IP läßt so keine Rückschlüsse zu.
- Verbindungen kommen i.d.R. über mehrere anonymisierende Hops hintereinander.
  - Strafverfolgung quer durch die Welt bei solchen Sachen praktisch aussichtslos.

# Doch warum waren Backdoor und Systemmanipulation nicht richtig erkennbar?

- Auf dem Server waren die wichtigen Systemprogramme durch Rootkit-Varianten ausgetauscht:

```
hostxxx:~# ls -la /bin
[...]
-rwxr-xr-x 1 root root    45384 15. Feb 2011  login
-rwxr-xr-x 1  122 obsrun  39696 28. Apr 2010  ls
-rwxr-xr-x 1 root root     5904 30. Okt 2011  lsmod
-rwxr-xr-x 1 root root    48864 28. Apr 2010  mkdir
-rwxr-xr-x 1 root root   110120 28. Apr 2010  mv
-rwxr-xr-x 1 root root   188328 15. Apr 2010  nano
-rwxr-xr-x 1  122 obsrun  54152 16. Mär 2009  netstat
-rwxr-xr-x 1 root root    15128 22. Mär 2010  nisdomainname
lrwxrwxrwx 1 root root       14 10. Aug 2012  pidof -> /sbin/killall5
-rwsr-xr-x 1 root root    34248 14. Okt 2010  ping
-rwsr-xr-x 1 root root    36640 14. Okt 2010  ping6
-rwxr-xr-x 1  122 obsrun  62920 16. Feb 2012  ps
-rwxr-xr-x 1 root root    31968 28. Apr 2010  pwd
```

Peer Heinlein <p.heinlein@heinlein-support.de>

# Wo wurde denn was ausgetauscht?

```
hostxxx:~# find -uid 122
./bin/ls
./bin/netstat
./bin/ps
./usr/bin/top
./usr/bin/find
./usr/bin/pstree
./usr/bin/md5sum
./sbin/ttymon
./sbin/ifconfig
./sbin/ttyload
```

# Jetzt ergeben auch die Fehlermeldungen Sinn...

```
hostxxx:~# cd .../
hostxxx:~/...# ls -la
ls: unrecognized prefix: rs
ls: unparsable value for LS_COLORS environment variable
total 32
drwxr-xr-x   3 root     root         4096 Dec 30 09:23 .
drwx------   9 root     root         4096 Jan  1 11:34 ..
drwx------   2 2112     2000         4096 Jan  1 10:52 .x
-rwxr-xr-x   1 root     root        17557 Jan 22  2011 mm
```

Peer Heinlein <p.heinlein@heinlein-support.de>

## Jetzt ergibt so manches Sinn...

- Wie sagte der Kunde nochmal am Telefon?

  *"Ich will eh weg von Server4You. Die Kiste ist lahm und bringt keine Leistung. Die haben das einfach nicht im Griff."*

- Mit "top" war nie etwas zu sehen...
- In Wirklichkeit hatte die Kiste > 100 ssh-Brute-Force-Prozesse & Co am laufen und ächzte unter Vollast...
- [Nochmal zur Klarstellung: Server4You als Hoster hatte damit nichts zu tun, die Kiste war top in Ordnung.]

Peer Heinlein <p.heinlein@heinlein-support.de>

## Und sagt der Kunde?

- Alle doof, außer Mutti.
- Server4You doof.
- Ex-Mitarbeiter doof.
- Angreifer doof.
- Welt doof.

- Später sagte der Kunde auch: Heinlein doof.
  Dazu gleich mehr :-)

# Tja, was für Schlüsse zieht man nun daraus?

- Kunde:
  Das verstehe ich nicht. Wenn der sich einloggen konnte dann mußte das doch mein Ex-Mitarbeiter sein.

- Ich:
  Naja, sie sehen ja, die machen Brute Force-Angriffe und raten massenhaft Passwörter. Wenn da mal was einfaches oder gar "test123" oder so gesetzt war, dann kommt man da schon rein.

Peer Heinlein <p.heinlein@heinlein-support.de>

Was antwortet der Kunde?

*Das Passwort kommt mir bekannt vor.*

Peer Heinlein <p.heinlein@heinlein-support.de>

## Und weiter?

- Auch später diskutierte der Kunde weiterhin darüber, dass das ein Ex-Mitarbeiter gewesen sein muß.

- Na gut.

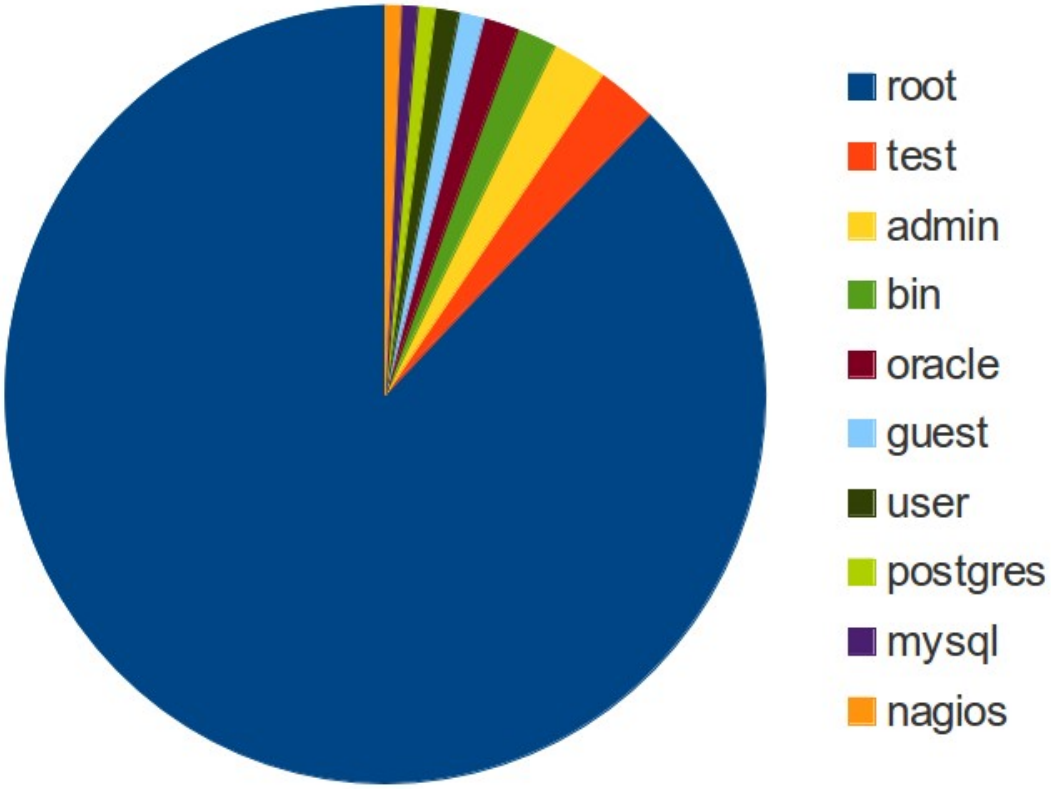
Peer Heinlein <p.heinlein@heinlein-support.de>

# Welche Passwörter hat er Angreifer eigentlich probiert?

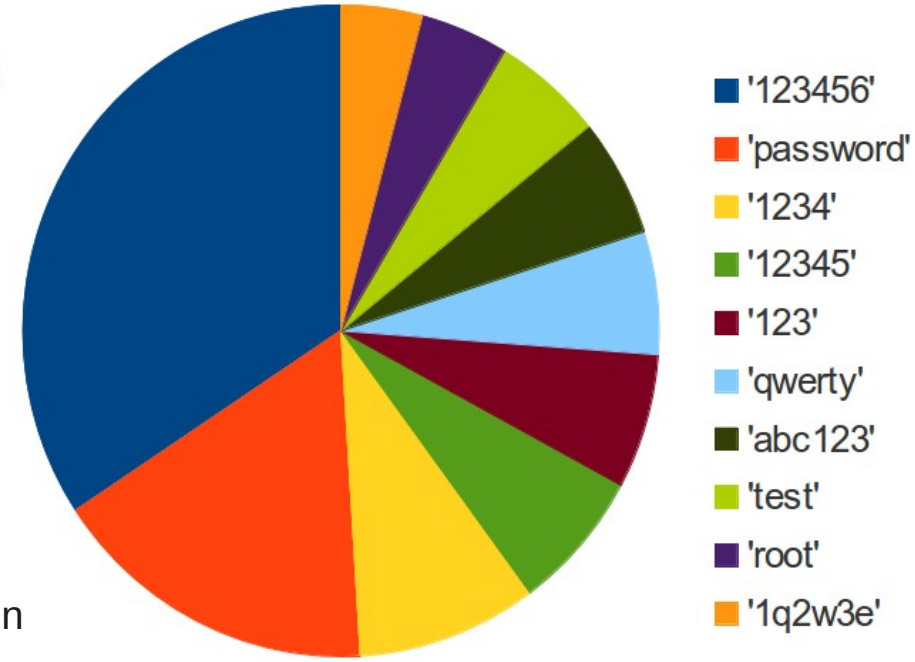
- root root
- root 123
- root qwerty
- root 12345678
- root 121212
- root adidas
- root passwd
- root qazwsx123
- root abc123
- root 1qaz2wsx
- root qazxsw2
- root toor
- root 111111
- root 123456
- root 1
- root root01
- root asterisk
- Root cisco

Peer Heinlein <p.heinlein@heinlein-support.de>

## Top 10: Angegriffene Benutzer




## Top 10: Passworte




Von: Andreas Bunten, Thorsten Voss u.a.
SSH-Angreifern mit Honeypots über die Schulter schauen

Peer Heinlein <p.heinlein@heinlein-support.de>

## Rekapitulieren wir mal...

- Ein Webshop-Server mit kompletter Mail-Installation
- Ein Webshop mit offenem, laufendem nmbd-/Samba-Dienst
- MySQL war frei im Internet erreichbar
- SSH war frei im Internet erreichbar
- Keine Firewall

Peer Heinlein <p.heinlein@heinlein-support.de>

# Und was lernen wir?

- root-Login war nicht unterbunden
- root-Passwort war nicht sicher genug
- 30.000 SSH-Brute-Force-Logins haben keinerlei Alarm oder Verdachtsmoment ausgelöst
- Keine Firewall hat Zugriff auf 22 oder Backdoor-Port 112 verhindert
  - Okay, Angreifer hatte eh root-Zugriff und hätte die FW anpassen können.
- Es gab eventuell mehrere Angreifer auf dem System – die ersten Dateien waren 23.12. – mangels Logfiles nicht mehr nachvollziehbar. Root-Passwortänderung aber erst 25.12.!

Peer Heinlein <p.heinlein@heinlein-support.de>

## Unser Fazit zum Kunden:

- Der Server ist ein Totalschaden und nicht mehr vertrauenswürdig.
- Sie müssen ihn definitiv ASAP neu aufsetzen
- Es können Kundendaten entführt worden sein
- Alle Zahlungsaktionen über den Server könnten kompromittiert worden sein
- Der Web-Content des Servers konnte kompromittiert worden sein
- Ihr jetziges Setup ist eine totale Katastrophe.
- Sie brauchen jemanden, der solche Kisten pflegen kann.
- Nehmen sie das bitte verdammt ernst!

Peer Heinlein <p.heinlein@heinlein-support.de>

# „Epilog“

Peer Heinlein <p.heinlein@heinlein-support.de>

## Und wie ging die Geschichte weiter:

- Kunde glaubte auch nach umfangreichen Telefonaten nicht, daß Ex-Mitarbeiter damit aller Wahrscheinlichkeit nichts zu tun hat.
- Wir stellten nur 2 x 2,5 Mannstunden Arbeitsleistung in Rechnung
  - Bis hierhin war's ja ganz nett und wir helfen gerne
  - Kunde hat kleinen Shop und hart verdientes Geld
  - Telefonberatung > 2h nicht berechnet
  - Nacharbeiten (Sylvester 4 Uhr!) nicht gesondert berechnet
- Kunde diskutiert über Rechnungshöhe.
- Server wird entgegen unserem Rat weiter betrieben.

Peer Heinlein <p.heinlein@heinlein-support.de>

# 6 Wochen später:

- Kunde zahlt nur Teilbetrag und schreibt uns auf 2 Seiten:
  - […] Weiter wird inzwischen geprüft, in wie weit uns bereits ein Schaden in Hinblick unseres Webshops […] entstanden ist, da dieser uns seit geraumer Zeit, trotz Ihrer Behebung der Schäden, nicht mehr zur Verfügung steht.
  - […] Dazu ist zu sagen, daß wir in den letzten Wochen eine komplette Neuinstallation vornehmen mussten.
  - […] Als Fachfirma sollten Sie wissen, dass wenn ein Server erst einmal gehackt ist, das er dann, ohne eine komplette Neuinstallation im WWW nicht mehr vertrauenswürdig ist!
- Kunde mindert um 50% und zahlt nur 2,5 Mannstunden
- Unsere Replik und letzte Zahlungsaufforderung blieb unbeantwortet.

Peer Heinlein <p.heinlein@heinlein-support.de>

Soviel dazu.

Peer Heinlein <p.heinlein@heinlein-support.de>

- Lust auf mehr?
- Unser Vortrag
  „Dem Hack keine Chance – LAMP-Server sicher betreiben“
  auf http://www.heinlein-support.de/vortrag

- Lust auf weniger?
  Wie wäre es mit qualifiziertem Server-Management durch uns?
  http://www.heinlein-support.de/server-management

- Unsere 24/7/365-Hotline: 030 / 40 505 - 110

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 - 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Totalschaden. Ein gehackter Server auf dem Seziertisch.
[CeBIT Forum Open Source 2013]
Peer Heinlein <p.heinlein@heinlein-support.de>


**Ja, diese Folien stehen auch als PDF im Netz...**

**http://www.heinlein-support.de/vortrag**

Peer Heinlein <p.heinlein@heinlein-support.de>

**Soweit, so gut.**

**Gleich sind Sie am Zug:**
**Fragen und Diskussionen!**

Peer Heinlein <p.heinlein@heinlein-support.de>

# Und nun...


- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

**Bis bald.**

heinlein


Peer Heinlein <p.heinlein@heinlein-support.de>

# Heinlein Support hilft bei allen Fragen rund um Linux-Server

## HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

## HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

## HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

## HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.