Analyse eines gehackten Webservers unter Linux

Portrait

- Georg Höllrigl
- HTL St. Pölten - Elektronik / Technische Informatik
- 8 Jahre Erfahrung als Systemadministrator
- FH Mittweida – Informationstechnik
-  XIDRAS GmbH
- Technischer Dienstleister, Domainverwaltung, Rechenzentrum in Wien und Amsterdam

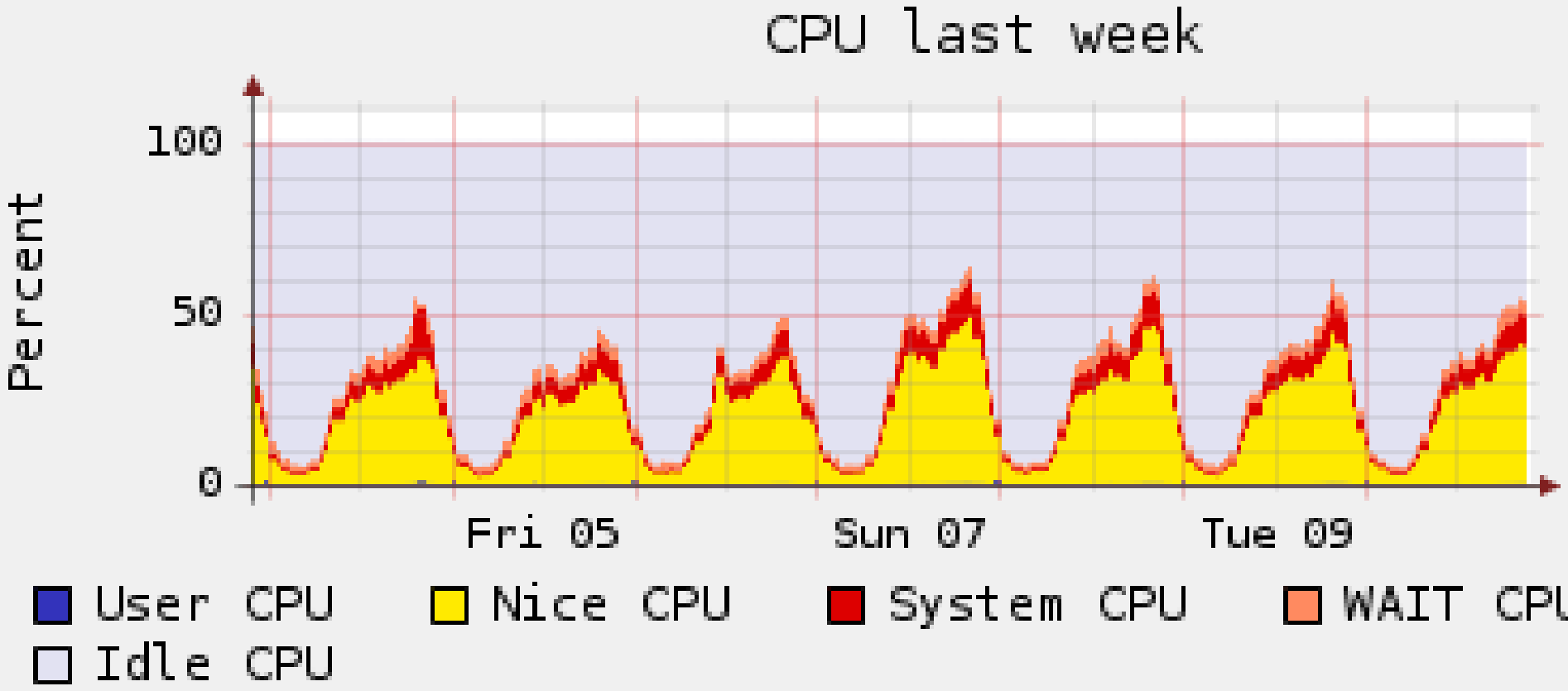
Gliederung

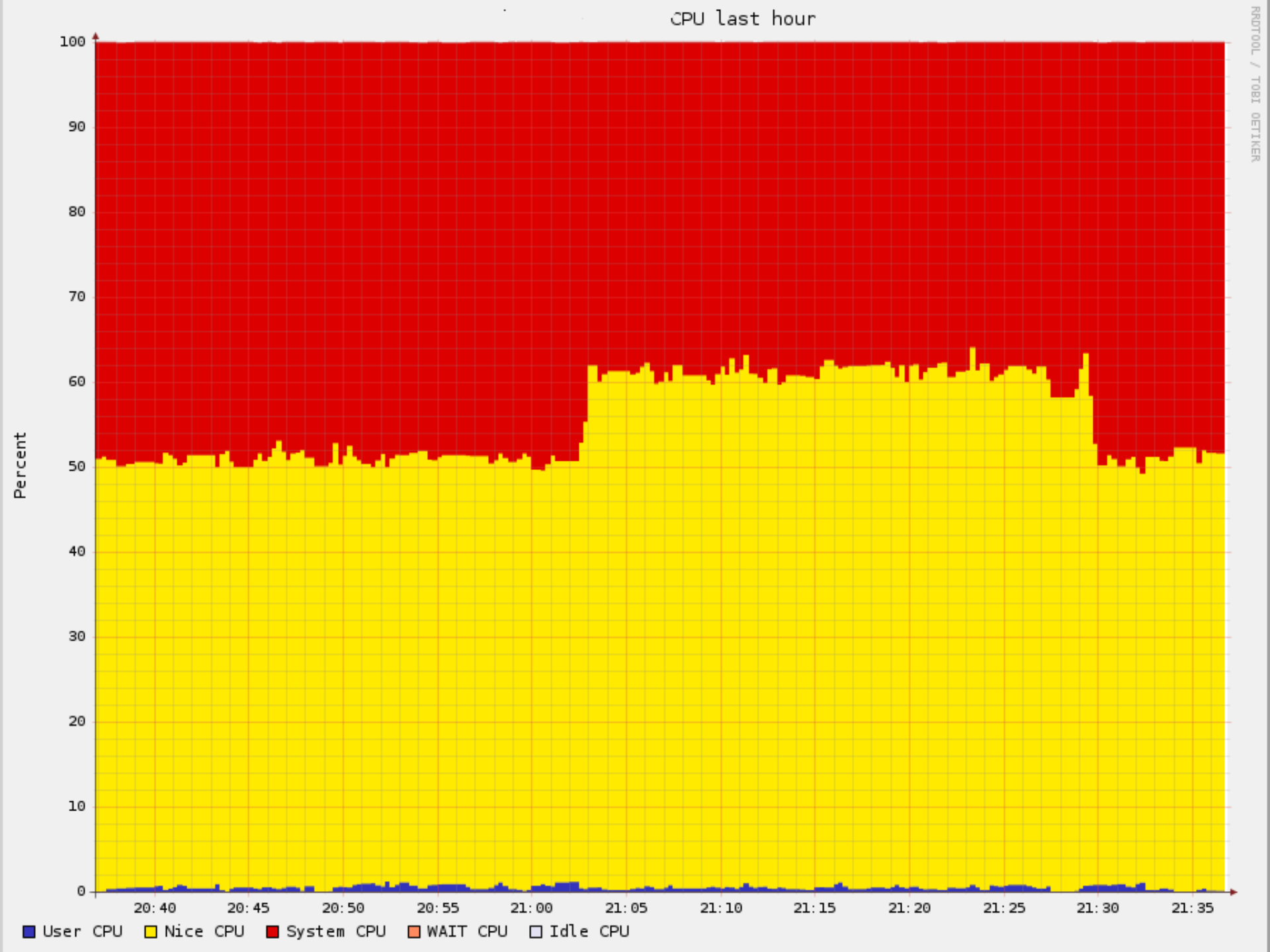
- Problemerkennung
- Alarmierung: rkhunter und chkrootkit
- Tools: lsof, strings, strace
- Was hat der Hacker alles am Server angestellt
- Was ist in den Logfiles zu finden?
- Wie wurde der Service wieder hergestellt?
- Neuinstallation

Problemerkennung

- Wie?

- Andauernde CPU Auslastung
- Festplatte voll
- Apache restart: port already in use
- rkhunter oder chkrootkit Alarmierung
- Beschwerde von Dritten


CPU last week
Percent
100
50
0
Fri 05
Sun 07
Tue 09
User CPU
Nice CPU
System CPU
WAIT CPU
Idle CPU


CPU last hour
Percent
100
90
80
70
60
50
40
30
20
10
0
20:40
20:45
20:50
20:55
21:00
21:05
21:10
21:15
21:20
21:25
21:30
21:35
User CPU
Nice CPU
System CPU
WAIT CPU
Idle CPU
RRDTOOL / TOBI OETIKER

rkhunter / chkrootkit

Found string 'fucknut' in file '/sbin/ttymon'. Possible rootkit: SHV5 Rootkit

Found string 'lamersucks' in file '/sbin/ttymon'. Possible rootkit: SHV5 Rootkit

Found string 'skillz' in file '/sbin/ttymon'. Possible rootkit: SHV5 Rootkit

Found string 'propert of SH' in file '/sbin/ttyload'. Possible rootkit: SHV5 Rootkit

Found string 'ttyload' in file '/etc/inittab'. Possible rootkit: Possible SHV5

Problemerkennung

- Was genau?

rs3418:/var/log # ls

ls: unrecognized prefix: do

ls: unparsable value for LS_COLORS environment variable

rcapache2 start

Starting httpd2 (prefork) (98)Address already in use: make_sock: could not bind to address [::]:80

(98)Address already in use: make_sock: could not bind to address 0.0.0.0:80

lsof

- Erstellt eine Liste offener Dateien und Ports

```
# lsof -i :80
COMMAND    PID   USER   FD   TYPE DEVICE SIZE
   NODE NAME
httpd2-pr  892 wwwrun    3u  IPv6  10414      TCP
   *:http (LISTEN)
httpd2-pr  893 wwwrun    3u  IPv6  10414      TCP
   *:http (LISTEN)
httpd2-pr  894 wwwrun    3u  IPv6  10414      TCP
   *:http (LISTEN)
```

255 17105 root 3u IPv6 11133028135
TCP *:80 (LISTEN)

255 17105 root 5u IPv6 11133028140
TCP *:443 (LISTEN)

255 17105 root 255u IPv4
11149127797 TCP *:1989 (LISTEN)

```
# lsof -p 17105
COMMAND   PID USER   FD   TYPE     DEVICE      SIZE
   NODE NAME
255     17105 root  cwd    DIR       8,3       696          2 /
255     17105 root  rtd    DIR       8,3       696          2 /
255     17105 root  txt    REG       8,3    652620
   14638336 /tmp/sh-CU2F1LKAQWG (deleted)
255     17105 root  mem    REG       0,0                    0
   [heap] (stat: No such file or
directory)
```

lsof - Praxistipps

- lsof braucht zu lange?
- lsof –P –n verwenden

- lsof –i :Port

- lsof –p PID

- lsof | grep Datei

```
wwwrun@hagrawuk:/tmp> ls -al
total 132156
drwxr-xr-x  2 root   root      4096 Nov  8 23:21
drwxrwxrwt 47 root   root     12288 Nov  8 23:25 .
drwxr-xr-x 28 root   root      4096 Nov  4 10:18 ..
drwxr-xr-x  2 root   root      4096 Nov  8 23:21 ...
drwxrwxrwt  2 root   root      4096 Jul 20 18:15 .ICE-uni
drwxrwxrwt  2 root   root      4096 Nov  4 10:20 .X11-uni
-r--r--r--  1 root   root        11 Nov  4 10:20 .X2-lock
-rw-rw-r--  1 wwwrun www         93 Nov 12  2009 .htacces
-rw-------  1 root   root       393 Jun  6  2007 .ifstat.
drwxr-xr-x  2 root   root      4096 Nov  4 10:18 .iroha_u
drwxr-xr-x  2 root   root      4096 Jan  8  2008 .webmin
drwxr-xr-x  2 root   root      4096 Nov 30  2008 1
-rw-r--r--  1 root   root        22 Jan 23  2009 1.txt
drwxr-xr-x  2 root   root      4096 Apr 15  2009 2
-rw-r--r--  1 root   root       371 Jul  8  2008 22463.ha
-rw-r--r--  1 root   root         0 Jul  8  2008 22463had
drwxr-xr-x  2 root   root      4096 Dec 19  2008 4
```

strings

 # cat hello.c

```
#include <stdio.h>
int main(void)
{ printf("Hallo Welt"); return(0); }
```

 # strings a.out

/lib/ld-linux.so.2

SuSESuSE

_Jv_RegisterClasses

__gmon_start__

libc.so.6

printf

_IO_stdin_used

__libc_start_main

GLIBC_2.0

PTRh

[^_]

Hallo Welt

strace

```
rs3418:/ # strace -p 17107
Process 17107 attached - interrupt to quit
[ Process PID=17107 runs in 32 bit mode. ]
restart_syscall(<... resuming interrupted call ...>) = 0
read(0, 0xffc8aea0, 1072)               = -1 EAGAIN
   (Resource temporarily unavailable)
time(NULL)                              = 1285327335
nanosleep({858993459200000,
   577765979979777072}, NULL) = 0
```

Was geben die logfiles her?

- dmesg
- /var/log/messages
- Apache access und error log
- /var/log/mail
- ~/.bash_history

[Wed Sep XX 22:56:28 2010] [notice] mod_fcgid: call /srv/www/vhosts/example.com/httpdocs/jasminesblog/index.php with wrapper /usr/bin/php-cgi5

[Wed Sep XX 22:56:28 2010] [notice] mod_fcgid: server /srv/www/vhosts/example.com/httpdocs/jasminesblog/index.php(20143) started

[Wed Sep XX 23:20:10 2010] [error] [client 208.80.XXX.XX] request failed: error reading the headers

[Wed Sep XX 23:21:18 2010] [error] [client 208.80.XXX.XX] request failed: error reading the headers

Empty input file

Empty input file

Ergebnisse aus den Logfiles

- nicht immer eindeutig
- nicht immer ergiebig
- „schuldige“ Domain über Error-Logs
- Veraltete Joomla-Installation

Was wurde am Server verändert?

- Manipulation der Log-Dateien
- Versteckte Unterordner mit Programmteilen
- IRC-Server
- Spam-Mail-Versand
- Backdoor über /etc/inittab

Wenn DEIN Server gehackt wurde, dann ist es nicht mehr DEIN Server!

- Sauberes System aufsetzten
- Backup einspielen
- Neues System besser absichern
- Sicherheitsupdates einspielen!

Danke