

(no title)

Ingo Blechschmidt

23. Juni 2005

## Inhaltsverzeichnis

0.0.1 John the Ripper . . . . . 1

### 0.0.1 John the Ripper

#### Mitschneiden

»**/mnt/warez/files/**«

Enthält Unterordner mit den Namen der Streams. In diesen Ordnern sind dann die mitgeschnittenen Dateien.

»**/mnt/warez/logs/**«

Die Log-Datei von streamripper, für jeden Stream. Escape-Sequenzen, die streamripper erzeugt, werden von log-cleaner automatisch weggeschnitten.

»**/mnt/warez/server-started**«

Existiert diese Datei, so läuft streamripper.

Wird benötigt von streamcd, um den streamd je nach Tageszeit zu starten oder zu stoppen.

»**/mnt/warez/streamd**«

Startet alle streamripper-Prozesse, unabhängig von der Tageszeit.

**»/mnt/warez/streamcd«**

Abhängig von der Tageszeit wird streamd aufgerufen, um streamripper zu starten oder zu stoppen. Wird automatisch alle fünf Minuten von cron aufgerufen.

**»/mnt/warez/log-cleaner«**

Löscht die Escape-Sequenzen in den streamripper-Logs. Wird jede halbe Stunde von cron aufgerufen.

**SSH-Tunnel**

»/home/ripper/tunneln.sh« baut einen Tunnel von »m19s28.vlinux.de:1235« zu »john:22« auf, und kümmert sich auch darum, dass der Tunnel automatisch wieder gestartet wird, wenn er mal down geht, etc. Wird automatisch von rc gestartet (»/etc/rc2.d/S99tunnler«).

Zugriff geht dann mit: »ssh -p 1235 root@m19s28.vlinux.de«. Aber: Man wird ständig seine »~/.ssh/known\_hosts« anpassen müssen, weil der Hostname der gleiche ist (m19), aber der sshd dahinter nicht. Abhilfe schafft folgender Eintrag in der »/etc/hosts«:

```
$ su -
Password:
# cat >> /etc/hosts
83.151.29.94    john.infothek    john
^D
# exit
$ ssh -p 1235 root@john
Password:
```