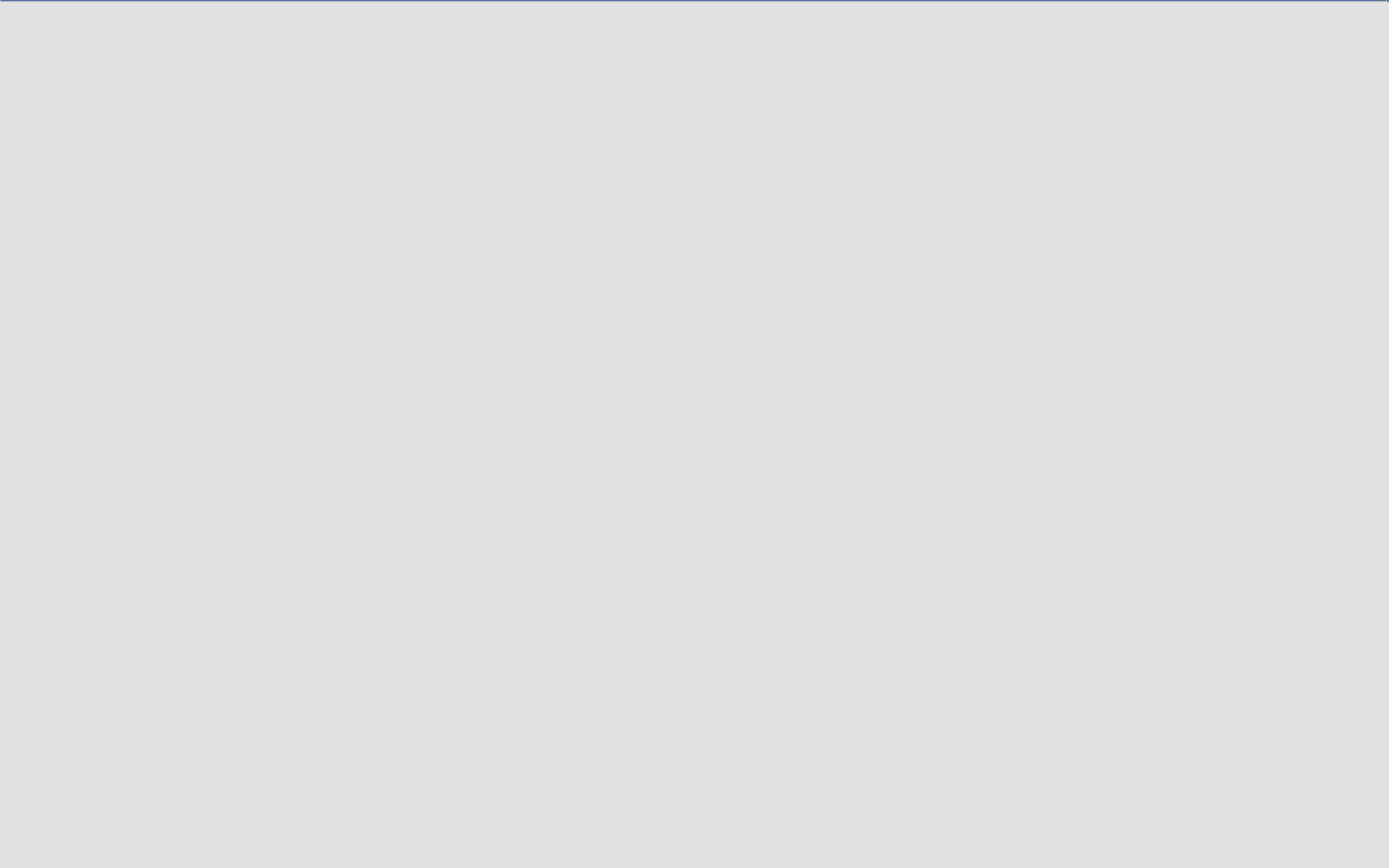


Einzelnen Beitrag anzeigen

Thema: [Loop-AES unter Linux \(Partition, Container, CD/DVD und Windows\)](#)

17.07.05, 00:18

#5



DaGrrr

Moderator



Registriert seit: Jul 2002

Beiträge: 1.767

Verschlüsseln der Swap-Partition mit loop-aes

Bei diesem Teilabschnitt gehe ich davon aus, das loop-aes bei dir eingerichtet ist und funktioniert.

Eine Swap-Partition oder auch Auslagerungsspeicher genannt, ist die Bezeichnung für Speicherplatz, der auf einer Festplatte eingerichtet wird, um scheinbar den verfügbaren Arbeitsspeicher des Systems zu vergrößern.

Wenn wir mit unserem System gearbeitet haben und auch unsere loop-aes Partition/Container genutzt haben, so könnten sich Daten auf der Swap-Partition

befinden und wären lesbar für jemanden der z.B. das Notebook stiehlt.

Da wir das gerne verhindern möchten, nun eine Erklärung, wie wir die Swap-Partition ebenfalls mit loop-aes verschlüsseln können.

Als erstes müssen wir folgenden Befehl ausführen, während wir uns in unserem util-linux Sourcerverzeichnis/mount befinden:

Code:

```
install -m 755 swapon /sbin
```

Da das Programm "swapon" ebenfalls vom loop-aes Patch gepatcht wurde, brauchen wir diese Datei.

Wir schalten die laufende Swap-Partition ab.

Code:

```
swapoff -a
```

Dabei werden alle Swap-Partitionen abgeschaltet, die in der /etc/fstab eingetragen sind.

Nun schreiben wir neue Informationen in die /etc/fstab:

Code:

```
/dev/hdXY none swap sw,loop=/dev/loop1,encryption=AES256 0 0
```

Da wie gesagt noch alte unverschlüsselte Daten sich auf der Swap befinden könnten, werden wir diese erstmal überschreiben:

Code:

```
dd if=/dev/zero of=/dev/hdXY bs=64k conv=notrunc  
mkswap /dev/hdXY
```

Nun starten wir unsere Swap wieder mit dem Befehl:

Code:

```
swapon -a
```

und führen danach

Code:

```
rm -rf /var/log/ksymoops
```

aus.

Bei loop-aes für eine Swap-Partition ist kein Passwort notwendig, da Zufallsschlüssel benutzt werden, der für die laufende Session gültig ist und bei einem Neustart des Systems oder aushängen und wieder einhängen der Swap neu generiert wird.

Nun ist die Swap-Partition ebenfalls mit loop-aes verschlüsselt.

Debian GNU/Linux SID / Kernel 2.6.16-SMP

[Private Linux Page](#) [Linuxserverforum](#) [MyBlog](#) [Debian Blog](#)

Geändert von DaGrrr (18.10.05 um 21:04 Uhr).

