Secure

[tmp] Verzeichniss mit noexec

HOW-TO: Mount /tmp mit noexec

Viele Leute die einen eigenen Webserver betreiben,
kennen das Problem mit sicherheit :-)

Es können im /tmp Verzeichniss beliebige Dateien ausgeführt werden.
Dies nutzen einige Scriptkiddys um sich Zugang zum Server zu verschaffen.

Diese Sicherheitslücke werden wir nun schließen indem wir ein neues Verzeichniss anlegen, in dem das ausführen von Proogrammen nicht erlaubt ist.

Dies schützt den Server vor den meisten exploits oder rootkits.

Nun gehts los:

Die folgenden Schritte kann man sich natürlich sparen, wenn man gleich beim aufsetzen des Servers dem tmp Verzeichniss eine eigene Partition zuteilt.

Zuerst erstellen wir uns ein 1000 MB große Datei für unsere /tmp Partition.
Wenn das zu klein ist, kann man es auch Problemlos vergrößern. Erhöht einfach den count=1000000 Wert.

```
cd /dev
```

```
dd if=/dev/zero of=tmpMnt bs=1024 count=1000000
```

Jetzt erstellen wir uns ein erweitertes Filesystem für unser tmpMnt Datei.

```
mke2fs /dev/tmpMnt
```

Nun sichern wir das vorhandene /tmp Verzeichniss.
Einige Programme legen symbolische Links oder Cache Dateien ins /tmp Verzeichniss.

```
cd /
```

```
cp -R /tmp /tmp_backup
```


(c) 2025 Michael Stender <webmaster@webmasterhilfe.de> | 2025-07-13 10:14
URL: http://faq.webmasterhilfe.de/index.php?action=faq&cat=7&id=21&artlang=de

Jetzt mounten wir das neue Filesystem.

```
mount -o loop,noexec,nosuid,rw /dev/tmpMnt /tmp
```

```
chmod 0777 /tmp
```

Inhalt vom gesicherten /tmp Verzeichniss zurückkopieren und Backup löschen.

```
cp -R /tmp_backup/* /tmp/
```

```
rm -rf /tmp_backup
```

Nun müssen wir die fstab ändern, damit das neue Verzeichniss nach dem neustarten des Server auch noch erreichbar ist.

```
mcedit /etc/fstab
```

Du siehst nun folgendes:

```
/dev/hda3           /                       ext3    defaults,usrquota
    1 1
/dev/hda1           /boot                   ext3    defaults     1 2
none                /dev/pts                devpts  gid=5,mode=620  0
0
none                /proc                   proc    defaults     0 0
none                /dev/shm                tmpfs   defaults     0 0
/dev/hda2           swap                    swap    defaults     0 0
```

Am ende fügst du dies hinzu:

```
/dev/tmpMnt         /tmp                    ext2    loop,noexec,nosuid
,rw  0 0
```

(WICHTIG: jeder space ist ein tab)

(c) 2025 Michael Stender <webmaster@webmasterhilfe.de> | 2025-07-13 10:14
URL: http://faq.webmasterhilfe.de/index.php?action=faq&cat=7&id=21&artlang=de

Secure

Das war es schon. Das ganze kann man dan ganz einfach überprüfen indem du eine Datei (test) im /tmp Verzeichniss mit folgendem Inhalt anlegst:

```
#!/bin/sh
ps
```

danach ein

```
chmod 755 /tmp/test
```

Und nun testen wir das ganze:

```
./test
```

```
bash: ./test: /bin/sh: bad interpreter: Keine Berechtigung
```

Unter Debian bekommt man leider Probleme beim einspielen von Updates (apt-get).

Dies kann man aber umgehen, indem man unter /etc/apt/ eine Datei apt.conf mit folgendem Inhalt angibt:

```
DPkg::Pre-Invoke {"mount -o remount,exec /tmp";};
DPkg::Post-Invoke {"mount -o remount /tmp";};
```

Das wars...

Eindeutige ID: #1020
Verfasser: Michael Stender
Letzte Änderung: 2010-11-17 02:28

(c) 2025 Michael Stender <webmaster@webmasterhilfe.de> | 2025-07-13 10:14
URL: http://faq.webmasterhilfe.de/index.php?action=faq&cat=7&id=21&artlang=de