

Menghapus Jejak Log Di Server Admin

Written by idnic

Tuesday, 11 September 2012 12:34 - Last Updated Tuesday, 11 September 2012 17:36

Â

Â

bagaimana cara agar si admin tidak mengira bahwa servernya pernah dimasuki dan diutak-atik seseorang lewat remote shell ssh. Sehingga siadmin tidak merubah-rubah password untuk kita gunakan pada penyusupan berikutnya.

Menghapus log juga bertujuan untuk tidak meninggalkan ip address yg bisa dilacak kepunyaanya oleh si admin.

Tutorial ini berkaitan dengan cara menghapus semua log yg mencatat aktifitas penyusup dalam sistem operasi linux.

Menghilangkan diri dari perintah last (perintah untuk melihat catatan semua user yg pernah login/logout baik local maupun remote) command yg digunakan adalah:

```
echo > /var/log/wtmp  
echo > /var/log/lastlog
```

Log-log yang lain yg perlu dihapus pake command:

```
echo > /var/log/messages  
echo > /var/log/secure  
echo > /var/log/maillog  
echo > /var/log/xferlog
```

Jangan lupa terakhir menghapus history shell command:

```
history -c
```

Menghapus Jejak Log Di Server Admin

Written by idnic

Tuesday, 11 September 2012 12:34 - Last Updated Tuesday, 11 September 2012 17:36

setelah itu jangan ketik apa-apa lagi, just **logout** or **ctrl+D**