الأداة faillog

يستطيع مدير النظام استعمال هذه الاداة بعد ان يقوم بعمل الاعدادت السابقة الخاص بالـpam_tally ، وتستخدم هذه الاداة لمعرفة عدد محاولات الدخول الخاطئة للمستخدمين حسب المثال التالي:

```
[root@linuxac ~]# faillog -u h4cker
Username   Failures  Maximum  Latest
h4cker          5        0      Wed Dec  5
11:16:30 +0300 2007 on tty1
```

استخدام الخيار -u لتحديد اسم المستخدم.
لاحظ في المثال السابق ان المتسخدم h4cker قد قام بعدة محاولات دخول خاطئة تسببت في قفل الحساب بشكل كامل. أي ان المستخدم لن يستطيع الدخول من الآن فصاعدا حتى لو قام بادخال كلمة المرور الصحيحة.

لعمل اعادة فتح للحساب كل ما عليك فعله هو استخدام الأمر :

```
faillog -u h4cker -r
```

ملاحظة: لا بد انك بدأت بالتساؤل إن كان هذا الأمر سيمنعني من تسجيل الدخول بالمستخدم الجذر root في حالة تكرار الدخول الخاطئ؟!؟! الجواب هو:

كلا ! لن يؤثر هذا الامر على المستخدم root .

خدمات الSSH و بعض النصائح.

تعتبر خدمة الصدفة الآمنة أو ما يطلق عليها بSecure Shell من اكثر خدمات الوصول عن بعد انتشارا و استخداما بين اوساط مدراء الأنظمة لما توفره هذه الخدمة من وصول آمن. لكن بعض الاعدادات البسيطة قد تساعد على زيادة مستوى الامان على خادمك بعمل اضافات بسيطة سناتي على ذكر البعض منها هنا.

-تغيير المنفذ الافتراضي لخدمات SSH

ترتبط خدمة الـSSH بشكل افتراضي مع المنفذ رقم ٢٢ على الخادم. وكون هذا المنفذ سيكون من أهم المنافذ التي سيجري تنفيذ عمليات مسح لها باستخدام port scanners مختلفة فإن اغلاق هذا المنفذ و استخدام منفذ آخر للوصول للخدمة سيؤدي الى تصعيب عملية كشف هذا المنفذ وخاصة عند استخدام اي من تلك البرامج.

الملف الخاص باعدادات خدمة الـ SSH هو

```
/etc/ssh/sshd_config
```

قم بتغيير السطر التالي في ملف الاعدادات من:

```
Port  22
```

ليصبح:

```
Port 51268
```

وعند محاولة الاتصال على خادمك كل ما عليك فعله هو استخدام الأمر ssh مع الخيار p لتحديد رقم المنفذ الذي تريد الاتصال عليه.