نوشته شده توسط root
پنجشنبه ، 6 خرداد 1389 ، 18:27 - آخرین بروزرسانی پنجشنبه ، 6 خرداد 1389 ، 19:12

فرض می کنیم من سیستم عامل FreeBSD را به عنوان یک سرور نصب کرده ام و سرویس های مختلفی مانند Apache و از بعد . ندارد وجود مشکلی و دهد می ادامه خود کار به خوبی به Server و ام کرده run آن روی بر را Samba و FTP مدتی می بینیم که Server به خوبی کار نمی کند و المکی المکی Crash می کند . می روم تک تک پروسه ها را با دقت بررسی می کنم . ظاهرا همه چیز درست است و مشکلی وجود ندارد و همه چیز درست است . به فایلی بر خورد می کنم که به آن شک می کنم و احساس می کنم این فایل قبلا به این صورت نبوده است و ممکن است در اثر فرآیندی دچار تغییر شده باشد . یک Backup از این فایل ندارم . این دست کاری ممکن است در اثر نصب یک برنامه جدید و یا در اثر هک شدن باشد . ممکن است کسی توانسته به سیستم من نفوذ کند و فایل را دستکاری کند و این باعث خرابی سیستم من شود .

در سیستم عامل FreeBSD برای اینکه بفمهمیم آیا فایل بر روی سیستم دچار تغییر و دستکاری شده است که منظور در اینجا فایل های system ی می باشد . برنامه پر قدرت aide به داد من می شد و من با این برنامه می توانم چک کنم که آیا فایل دچار تغییر شده است و این به من کمک می کند تا برای رفع مشکل وقت کمتری را صرف کنم .

از این برنامه برای بررسی هک شدن نیز می توان استفاده کرد .

.داد قرار بررسی مورد را سیستم به نفوذ آن با توان می و کرد ترجمه نفوذ تشخیص پیشرفته برنامه توان می را Aide

اما نکاتی برای کار کردن با این برنامه وجود دارد :

۱- این برنامه بعد از نصب سیستم عامل و برنامه های مورد نیاز نصب شود و به اصطلاح فوری بعد از RUN شدن سیستم نصب باید گردد . نه بعد از این که سیستم Crash یا Hack شد . که دیگر به درد نمی خورد .

۲- لازم است هر چند یکبار Database برنامه Aide را جدید یا Update نمود تا و Database ها قدیمی را پاک کرد .

۳- اگر چنانچه این برنامه به شما گزارش دارد که یک فایل تغییر کرده است این به معنی هک شدن نمی باشد . این برنامه یک شناسنامه از فایل مورد نظر برای خود می سازد و آن را ذخیره می کند در Database و بعدا فایل را با آن Database مقایسه می کند . اگر ببینید مشخصات جدید با مشخصات قدیم سازگاری ندارد گزارش می دهد که این فایل دچار تغییر شده

است . این تغییر ممکن است در اثر Hack شدن رخ داده باشد . ممکن است خود سیستم تغییراتی در آن ایجاد کرده باشد . مثلا من قبلا فرض می کنیم ورژن ۴.۷ برنامه MC یا commander Midnight را نصب کرده ام و برنامه aide مشخصات این برنامه را برای خود ذخیره کرده است و من الان ورژن ۴.۷.۵ را نصب کرده ام . خوب الان اگر Aide را Run کنم چون مشخصات MC قدیمی را دارد و مشخصات MC جدید را ندارد . پس خیال می کند که بله این فایل مربوط به MC دچار تغییر شده است . پس لازم است هر چند یک وقت Database برنامه جالب Aide را Update کنیم .

برای نصب این برنامه در FreeBSD در ترمینال یا محیط متنی دستورهای زیر را تایپ می کنیم .

```
# cd /usr/ports/security/aide
# make install clean
```

با دستور های بالا این برنامه نصب می شود . خوب حالا به شاخه زیر می رویم

/usr/local/etc/

و دستور زیر را تایپ می کنیم

cp /usr/local/etc/aide.conf.sample /var/db/aide/aide.conf

برنامه Aide در هنگام نصب یک فایل conf هم نصب می کند که در این فایل conf تعریف شده است که از چه فایل های شناسنامه یا مشخصات ثبت گردد . که با دستور بالا می گوییم از همان فایل conf پیش فرض یا Default استفاده گردد.

خوب حالا به شاخه زیر می رویم

/var/db/aide

و دستور زیر را تایپ می کنیم

aide --init

این دستور باعث می شود که این برنامه با توجه به فایل conf یک Database از فایل های که در فایل Conf تعریف شده است تهیه کند . آن را در این شاخه نگهداری کند . این فرآیند ممکن است زمان بر باشد .

پس از تهیه Database حالی کافی است دستور زیر را در ترمینال تایپ کنم

aide --check

این دستور فایل ها را با Database **مقایسه می کند و ممکن است خروجی شبیه به زیر به شما بدهد .**

File /usr/local/share/claws-mail/themes/Everaldo_Kids/drafts_open_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/inbox_close_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/outbox_open_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/inbox_open_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/drafts_close.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/outbox_close_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/dir_close_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/trash_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/trash_open_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/linewrapcurrent.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/dir_open_hrm.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/inbox_close.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/dir_noselect.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/dir_close.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/outbox_close.png in databases has different attributes، bbf،1bbd File /usr/local/share/claws-mail/themes/Everaldo_Kids/queue_close_hrm.png in databases has different attributes، bbf،1bbd

خوب می بینم که چه فایل های دچار تغییر شده است و این تغییر در چه نوعی است

ممکن است خروجی به شکل زیر باشد

Summary: Total number of files: 269340 Added files: 50041 Removed files: 28784
Changed files: 99043

خوب می بنیم که 269340 **فایل داشته ایم که** 99043 **آنها دچار تغییر شده اند و عده ای هم پاک شده اند .**

ممکن است خروجی به شکل زیر باشد

changed: /usr/local/share/pixmaps/pidgin/emotes/default/brb.png

خوب به من می گوید که فایل png.brb **دچار تغییر شده و هزاران گزارش دیگر . جالب نیست**

من حدود ۲ ماه پیش این برنامه را نصب کرده ام و الان یک گزارش ۴۰ مگا بایتی درباره تغییرات به من می دهد و این عالی است

حتما لازم است که Database **این برنامه را** Update **کنیم تا تغییرات بعد از آخرین** Update **را را نیز داشته باشد کافی است دستور زیر را اجرا کنم**

aide --update

برای کسانی که Server **های پر ریسک دارند این برنامه لازم است.**