Advanced Intrusion Detection Environment

السلام عليكم ورحمة الله وبركاته

كيف أحوال الشباب إن شاء الله الجميع بخير وعافية ... اليوم قلت أكتب عن **AIDE** والذي هو إختصار لـ " **Advanced Intrusion Detection Environment**" وظيفته هي التحقق من سلامة الملفات **File Integrity** Checker الموجودة على النظام، طبعاً هنا أتكلم عن جنو/لينوكس :) يتم ذلك من خلال أخذ صورة **snapshot** للنظام في بداية تشغيلك له ومن ثم تصبح هي النقطة التي يتم بناء المقارنة عليها، أي في المستقبل عندما تشك بوجود حاجة غريبة أو تشك بإنه ربما قام أحد المخترقين بتنفيذ **exploit** على أو قام بتنصيب **RootKit** أو **Trojan** داخل النظام فإنك تستطيع مقارنة الملفات التي كنت قد أخذت لها **snapshot** مع الملفات الحالية وبالتالي تعرف إذا كانت هذه الملفات قد تغييرت أم لا ...

أول حاجة لنقم بتحميله من موقع **sourceforge**:
- تحميل aide

أيضاً سنحتاج الى مكتبة إسمها **mhash**، أيضاً قم بتحميلها من موقع **sourceforge**:
- تحميل mhash

الآن لنقم بتركيب mhash على نظامنا:
كود:

```
tar xzvf mhash-version.tar.gz
cd mhash-version
./configure
make
su -
cd /path2/mhash-version
make install
```

السبب في تنصيبنا لمكتبة mhash في البداية هي كما ذكرت لكم بالأعلى بإنها أحد متطلبات تنصيب **aide** على النظام ... لنقم الآن بتنصيب **aide** على النظام من خلال أتباع نفس الخطوات السابقة:
كود:

```
tar xzvf aide-version.tar.gz
cd aide-version
./configure
make
su -
cd /path2/aide-version
make install
```

الآن بما إننا سنقوم بإستعمال برنامج له علاقة بسلامة الملفات والتحقق منها File Integrity Checker، من الظرورة أن نقوم بأخذ الـ **md5** للبرنامج نفسه، فمن يدري ربما يتم عمل تبديل للبرنامج نفسه وبالتالي يتم التغطية عن جميع التغييرات التي قد تكون حصلت على الملفات الموجودة ... لعمل ذلك عليك أن تعرف أين يوجد برنامج **aide** أي أين تم تنصيب البرنامج التنفيذه حقه ... تستطيع معرفة ذلك من خلال قراءة البيانات التي ظهرت على الشاشة لديك حين قمت بعمل **make install** أو من خلال تنفيذ الأمر:

كود:

```
which aide
```

على كل حال المسار عندي هو:
كود:

```
/usr/bin/aide
```

الآن لنقوم بأخذ الـ md5 له من خلال تنفيذ الأمر التالي:
كود:

```
md5sum /usr/bin/aide
```

قم بحفظ الناتج في ملف وفي مكان لا يستطيع أحد الوصول أليه مثلا في جيبك :) أي ما أقصده أن تحتفظ به مثلا على **USB** أو **CD** وبالتالي هو بعيد المنال عن الناس ... طبعاً هناك ملاحظات أخرى سأذكرها في وقتها وهي مهمة جداً ... بعد عمل الكومبايل للبرنامج وتنصيبه ستجد في المجلد الأساسي الذي عملت منه الـ **compile** مجلد الـ **src** فيه ملف أسمه **aide** ... من خلاله أيضاً تستطيع أن تتأكد أكثر من سلامة الملف الذي قمت بتركيبه وذلك من خلال مقارنة الـ **md5** له مع الـ **md5** الخاصة بالملف الذي قمت بتركيبه في الخطوات السابقة ...

الآن لنفتح الملف الخاص بإعدادات **aide** ونلقي نظرة عليه ... أذهب الى:
كود:

```
vi /etc/aide.conf
```

- يوجد في الملف هذا متغييرات، **macros**، و الملفات/المجلدات التي نريد مراقبتها.
أولاً: المتغيير مثل:
كود:

```
@@define TOPDIR /home/user/
```

ثانياً: الـ **macro** مثل:
كود:

```
@@ifndef TOPDIR
@@define TOPDIR /
@@endif
```

حيث هنا قمنا بتعريف المجلد الذي سيكون المجلد الأب أو العلوي لباقي المجلدات.
ثالثاً: الملفات/المجلدات التي نريد مراقبتها مثل:
كود:

```
/etc R
```

- قاعدة البيانات الخاصة به هي: **aide.db.new** ويختلف مكان تخزينها من توزيعة الى أخرى وأيضاً لا ننسى بإنك تستطيع تغيير المسار الخاص بها وأيضاً إسم هذه القاعدة.

- تستطيع ان تحدد ما هي الـ **attributes** التي تريد **aide** أن يقوم بمراقبتها، مثل: permissions, atime, ctime, size, , user, group, md5hashes, mtime, inodes وغيرها.

- الجميل بالأمر إن **aide** لا يدعم **md5 hashes** فقط، وإنما يدعم **sha1** و **rmd160** و **tiger** و **crc32** وغيرها.

- أيضاً تستطيع أن تقوم بإستعمال أكثر من خيار للمراقبة وذلك من خلال إستعمال الخيارات التي تدل على خيارات متعددة مثل **R** حيث إنها تدل على إنك تريد مراقبة كل من:
p+i+n+u+g+s+m+c+md5 وكل واحدة موجود في ملف الـ **conf**. ماذا تعني. إستخدام هذه الطريقة **R** سيسهل علينا الكثير من الأمور سنراها في الشرح.

على الرغم من إنك تستطيع من خلال الخيارات التي يوفرها **AIDE** أن تقوم بعملية مراقبة للملفات التي تتغيير بشكل مستمر مثل ملفات السجلات **Log Files** إلا إنه يفضل إستعمال البرنامج **AIDE** لمراقبة الملفات التي لا تتغيير بشكل مستمر مثل ملفات الإعدادات الخاصة بالخدمات والملفات التشغيلية والأدوات ... وذلك لأنه مراقبة السجلات **Log** يجب أن تكون من وظائفك أنت مدير النظام أو وظيفة البرامج المعنية التي تهتم بقراءة السجلات **Log** مثل **IDS** وغيرها.

سؤال: لماذا لا يفضل إستعمال أو مراقبة الـ atime والذي هو Access Time بالرجوع لـ **aide** ؟
الجواب: سأتركه لكم للتفكير أو للتجربة ومعرفة السبب !!!

صراحة هناك خيارات كثيرة جداً للبرنامج لا أريد أن أقوم بشرحها كلها ويمكنك ان تتعرف عليها بمجرد قراءتها وقراءة ملفات المساعدة الخاصة بالبرنامج ولهذا سأدخل مباشرة الى بعض الخيارات التي سأقوم بإستعمالها في هذا الشرح.

الآن لو نفرض تريد أن تقوم بمراقبة المجلد **etc/** وكل ما هو في داخله، قم بوضع السطر التالي:
كود:

```
/etc R
```

بعد الجملة **Selection regexp rule.**

أول حاجة سنقوم بها بعد أن قمنا بعمل الاعدادات المطلوبة هي بناء قاعدة البيانات، ويمكننا عمل ذلك من خلال:
كود:

```
aide --init
```

إذا كنت تريد أن تقوم ببناء قاعدة البيانات بناءاً على إعدادات غير التي في المجلد الخاص بالبرنامج **aide**، وهذا الملف الخاص بالإعدادات موجود في مجلد آخر لنفرض في المجلد الرئيسي للمستخدم الذي تستعمله، ولنفرض هو **user** نقوم ببناء قاعدة البيانات بهذا الشكل:
كود:

```
aide -c /home/user/aide.conf --init
```

بعد أن تنتهي من تنفيذ هذا الأمر سيخبرك **aide** بإنه تم تهيئة القاعدة. للتأكد سترى بإنه تم خلق ملف إسمه **aide.db.new**. طبعاً هذه العملية ستأخذ بعض الوقت وذلك لأنه سيقوم ببناء القاعدة بناءاً على جميع المحتويات للمجلد **etc/** ولهذا قد تأخذ بعض الوقت للإنتهاء، ليس الكثير جداً. بعد أن قمت بتنفيذ الامر بالأعلى الأن تستطيع أن تقوم مثلا بقراءة محتوى الملف **aide.db.new** وذلك لأنه عبارة عن ملف نصي **Text File**. أفتح الملف أو قم مثلاً بالبحث عن السطور الخاصة بالملف **etc/resolv.conf/** وقارنها مع ناتج أمر الـ **stat** للملف نفسه. مثلاً:
كود:

```
stat /etc/resolv.conf
```

الناتج:
كود:

```
binary@rul3z:~> stat /etc/resolv.conf
  File: `/etc/resolv.conf'
  Size: 68              Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 1452487     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2008-06-15 23:55:45.000000000 +0300
Modify: 2008-06-07 17:00:22.000000000 +0300
Change: 2008-06-07 17:00:22.000000000 +0300
```

الآن قارن هذه المعلومات مع التي قام بتسجيلها **aide** في قاعدة البيانات الخاصة به، مثلاً بالنسبة للملف هذا كما نره حجمه 68 أنظر الى ما قام تسجيله **aide** ستجده قام بتسجيل هذه القيمة أيضاً، أيضاً مثلا أنظر الى رقم الـ **Inode** للملف هي **1452487** وأنظر لما سجله **aide** ستجده نفس الشي وهكذا. طبعاً **aide** سيسجل وفقاً للخيارات التي قمنا بإعطاءها له في السطر الذي كتبناه كما تذكرون
كود:

```
/etc R
```

في ملف الإعدادات حق **aide** ولا تنسو بإن **R** تعني **p+i+n+u+g+s+m+c+md5**. إذن نستطيع القول بإن أغلب ما قام بستجيله **aide** أتت من ناتج الأمر **stat** بإستثناء الـ **Hashes** والتي ستكون ناتج الأمر **md5sum**.

الآن لا تقم بأي تغيير أو شيء على الملفات الموجودة داخل المجلد **etc/** وذلك لكي نقوم بعمل أول تجربة لنا بإستعمال **aide**. الآن قم بتشغيل **aide** ولكن هذه المرة بإستخدام خاصية الفحص **check** ولنرى هل سيتعرف **aide** على التغييرات التي قمنا بها (والتي بالحقيقة هنا لم نقم بعمل أية تغييرات)، المهم لنجرب ونرى ماذا سيحصل:
كود:

```
aide --check
```

إن كنت تستعمل ملف إعدادات موجود في مكان آخر لا تنسى أن تمرره لـ **aide** من خلال الخيار c كما عملنا في السابق. بعد أن ينتهي من عملية الفحص سيخبرنا بإنه:

All files match AIDE database. Looks okay

أي إن جميع الملفات (التي بداخل المجلد **etc/** في مثالنا هذا) مطابقة لقاعدة البيانات وبهذا نعرف بإنه لا يوجد أو لم تحصل أي تغييرات على الملفات. طبعا في حالة كان هذا الجهاز هو خادم معيين سيكون شي ممتاز ومريح للأعصاب بإنك عرفت بإنه للحين لم يتم التلاعب في ملفات النظام لديك.

طيب الآن لنقوم بعمل تغيير بسيط على أي من الملفات الموجودة داخل المجلد **etc/** لنفرض قم بإضافة **nameserver** جديد الى الملف **resolv.conf**. نفذ الأمر التالي لكي نقوم بتجربة aide مرة أخرى ولكن هذه المرة بوجود ملف تم التعديل عليه. نفذ التالي:
كود:

```
echo "nameserver 192.168.0.22" >> /etc/resolv.conf
```

أو قم بتفعيل/إيقاف خاصية التمرير أو الـ **routing** من خلال التعديل على ملف **sysctl.conf**، إن كانت فعالة "**1**" أعملها غير فعالة "**0**" أو العكس، نحن فقط نريد أن نعمل أي تغيير لكي نرى النتائج التي سيعطينا إياها aide. بعد أن قمت بأي تعديلات تريدها، قم بتشغيل **aide** مرة أخرى بإستعمال خاصية الفحص **check** كالتالي:
كود:

```
aide --check
```

الآن سيخبرنا بإنه يوجد ملفات تم التعديل عليها وسيعطينا مقارنة بين الخصائص الحالية للملف بعد التعديل وبين الخصائص للملف قبل التعديل والتي هي مسجلة في قاعدة البيانات الخاصة بـ **aide**. من ظمن هذه التغييرات هنا ستكون الـ **md5** للملف وذلك لأنه نحن قمنا بمراقبة هذه الخاصية في الملفات، وأيضاً أي تغيير ولو بحرف واحد على الملف سيعرض الـ **md5 hash** للتغيير. طبعاً كل شي سيتم عرضه لك على شكل إحصائيات ومقارنات جداً سهلة قراءتها ...

سؤال: لو قمت بعمل تعديل على ملف **etc/hosts/** فقط، وقمت بعدها بعمل فحص من خلال **aide** لماذا سيقول لك بإنك قمت بالتعديل على ملفين وليس واحد؟
الجواب: أكتشفه بنفسك.

سؤال: ماذا لو تم إضافة ملف الى المجلد etc ؟
الجواب: أكتشفه بنفسك.

الآن لنفرض الحالة الطبيعية وهي أن تقوم أنت بعمل مثل التغييرات التي عملناها بالاعلى، ما سيحصل عند قيامك بالفحص بـ **aide** هو إنه سيخبرك بإنه الفحص وجد التغييرات الفلانية 1 2 3 4، والتي هي تغييرات أنت قمت بها. هنا نقوم بإخبار او تبليغ (أو أختر أي كلمة مناسبة ليتم وضعها هنا) **aide** بإنه هذه الخيارات طبيعية قم بإضافتها الى القاعدة، أي قم بتعديل القاعدة الخاصة بك على ضوء التغييرات التي هي موجودة حالياً. للقيام بذلك لنقم بعملية تأكد من إن التعديلات حصلت على الملفات التي قمنا نحن بالتعديل عليها فقط، ولهذا ننفذ الأمر:
كود:

```
aide --check
```

وبعد أن نتأكد بإن فعلا هذه التعديلات هي ما قمنا به نحن، نقوم بعمل التالي للتحديث:
كود:

```
aide --update
```

هنا سيقوم **aide** بتحديث قاعدة البيانات التي لديه وبالتالي في المرات القادمة سيتم المقارنة بناءاً على القاعدة الجديدة التي قمنا بتحديثها الحين.

الآن هناك مشكلة، وهي بوجود بعض الملفات بداخل المجلد **etc** تتغيير بعد عمل إعادة تشغيل، طبعاً هذه الملفات تختلف من نظام الى آخر. كيف سنقوم بمراقبة هذه الملفات إذن؟ الجواب هو إنني ذكرت بإنه يفضل مراقبة الملفات التي لا تتغيير بإستمرار أو ربما لا تتغيير نهائياً وهنا لا أقصد فقط الملفات التي بداخل المجلد etc لا، وإنما يفضل مراقبة الملفات التي بداخل المجلدات التالية أيضاً: **bin** و **sbin** و **usr** و **lib** و **boot** الذي يحتوي على النواة **Kernel** ولا يجب أن يتغيير بإستمرار وبالإضافة الى بعض الملفات الموجودة في المجلد **etc** أو كلها، حسب ما تحتاجه.

لهذا لنقم بإضافة السطور التالية، أسفل السطر الذي قمنا بإضافته سابقاً ليصبح لدينا كالتالي:
كود:

```
/etc R
/boot R
/bin R
/sbin R
/lib R
/usr R
```

هكذا نكون قد حددنا مراقبة هذه المجلدات وجميع الملفات/المجلدات التي بداخلها بشكل **Recursive** ... إن كنت تريد أن تقوم بتحديد جزء من مجلد هنا سنحتاج الى إستعمال إمكانيات الـ **regex**. مثلاً تريد أن يقوم **aide** بمراقبة الملفات التي بداخل المجلد **bin** مباشرة فقط وليست التي بداخل مجلدات بداخل هذا المجلد تستطيع أن تقوم بعمل ذلك من خلال تعديل السطر الخاص بالمجلد **bin** ليصبح هكذا:
كود:

```
/bin$ R
```

ولو كنت تريد أن تقوم بتحديد ملفات معينة للمراقبة ولنفرض تنتهي بالحروف **co** نستطيع عمل ذلك من خلال التالي:
كود:

```
/lib/*.co
```

أيضاً تستطيع أن تقوم بتحديد المجلد العام للمراقبة وتقوم بعد ذلك بإختيار المجلدات التي لا تريد مراقبتها والتي تقع أسفل هذا المجلد، مثلا لو نفرض تريد مراقبة المجلد / كله ومن ثم تقوم بعمل **exclude** استخراج لمجلدات معينة من هذه المراقبة يتم عمل ذلك من خلال السطور التالية:
كود:

```
/ R
!/var
!/tmp
!/home
```

وهكذا قمنا بمراقبة جميع ملفات النظام بإستثناء المجلدات التي قمنا بوضع الاشارة ! قبلها. إذن من هذا نفهم بإن أي مجلد لا نريد مراقبة محتواه نضع العلامة ! قبله.

سؤال: عندما نقوم بتغييرات معينة أو تغيير ملف الإعدادات، هل نستطيع أن نقوم بحذف القاعدة rm لها ومن ثم تشغيل **aide** وكأننا نقوم بتشغيله لأول مرة وذلك لبناء قاعدة جديدة؟ أم نستطيع أن نقوم بعمل **update** لها فقط؟
الجواب: قم بالتجربة أنت !!!

الآن بعد أن قمت بأخذ **snapshot** من النظام الذي لديك، تستطيع أن تقوم بنقل (حذف) البرنامج **aide** وملف الأعداد له والقاعدة التي قمت ببناءها الى مكان أمين ويكون قابل للقراءة فقط **Read Only**. أفضل طريقة لعمل ذلك هي نقل الملفات الى قرص **CD** العادي مثلا وذلك لانك تستطيع الكتابة عليه لمرة واحدة وبالتالي لن يستطيع أحد أن يقوم بتغيير البيانات التي عليه ... بهذه الطريقة قمنا بإخفاء الآثار لوجود البرنامج **aide**.

في حالة أردت عمل فحص للنظام مرة أخرى بناءاً على القاعدة التي قمت بالإحتفاظ بها عليك أن تقوم بنسخ ملف الأعدادات الى مجلد معيين وعليك أن تعدل قيمة المتغيير في الملف نفسه ليشير الى المسار الصحيح لوجود ملف الإعدادات، لا تنسى ذلك.

بعد أن أنتهينا من كل تنصيب ومن ثم تشغيل **aide** وأخذ ملف القاعدة وباقي الملفات المهمة، عندما تشعر بإن النظام لديك قد يكون تعرض الى إختراق أو تم التلاعب به، أدخل القرص **CD** وقم بتشغيل **aide** مرة أخرى مع تمرير ملف الإعداد الذي وضعناه على الـ **CD** وذلك ليقوم بالفحص والتأكد من سلامة جميع الملفات التي على النظام. إن كنت تريد أن تعقد المسألة أكثر على المخترقين في إمكانية إخفاء آثارهم وإمكانية إكتشافك لهذا التلاعب تستطيع أن تقوم بإستعمال أو الإعتماد على أكثر من **hash** في نفس الوقت مثلاً **md5** و **sha1** وهكذا. بالنهاية حتى أشطر المخترقين سيقعون في قبضة **aide**.

ملاحظة:
- الإختصار **FIC** تعني **File Integrity Checker**.

الموقع الرسمي للبرنامج

تقبلوا تحياتي الحارة ...
ودمتم بود جميعاً ...