السلام عليكم ورحمة الله وبركاته ...

دليل ملفات الـ Log

موضوعي لهذا اليوم أجده مهم للمحترفين وللمستخدمين العاديين ... ولم أجد أحد صراحة تكلم عنه سابقا ... ولا حتى فكر في السؤال عنه ولهذا ما سأتناول في هذا الموضوع تصنيف ملفات الـ Log وكيفية التعامل معها وفهم محتويات كل واحد منها ... وأيضا الطريقة التي يكتب النظام ملاحظاته في هذه الملفات ...

أولا: ما هو ملف الـ Log ؟

هو عبارة عن ملف يتم تدوين في الملاحظات حول العمليات التي يجريها النظام ... مثل تشغيل الخدمات كالـ ftp وتسجيل حالات الدخول والخروج للنظام ... وغيرها من الأمور التي سنذكرها لاحقا ...

ثانيا: ما هو المجلد الرئيسي لهذه الملفات ؟

المجلد الرئيسي لها هو /var/log

ثالثا: ما هي الملفات الرئيسية التي بداخل هذا المجلد ؟

boot.msg
firewall
lastlog
mail
messages
wtmp

والمجلدات التي في داخله كثيرة ... أهمها هي:

YaST2
cups
samba
squid

وغيرها الكثير لكن هذه أهمها أو أهم ما سأقوم بشرحه ...

رابعا: لقد سردت لنا الكثير من الملفات والمجلدات فما هو عمل كل واحد منهم ؟

نعم سأذكر كل ملف ومجلد وماذا ممكن أن تجد بداخله...

1- ملف الـ boot.msg

هذا هو الملف الذي يتم تخزين فيه جميع الأمور التي حصلت أثناء عملية الإقلاع للنظام ... من لحظة ما يتحمل الكيرنل وباقي الأمور التي تحصل عند الإقلاع من تعريف القطع المثبته لديك ... ولكن بسبب ظهورها بسرعة على الشاشة أثناء الإقلاع فلا تحصل على فرصة الى معرفة ماذا حصل ... خاصة إذا دخلت النظام ولم تجد مثلا جهاز قام بالعمل بشكل صحيح ... فكيك ستعرف إنه الكيرنل تعرف عليه أصلا ؟ من هنا ... أي هذا الملف يسجل جميع عملايات الإقلاع وجميع عمليات التي يقوم بها الكيرنل ... أيضا يمكنك أن تعرض محتويات هذا الملف من خلال الأمر dmesg

2- ملف الـ firewall

هذا الملف يتم تسجيل فيه عمليات التي تحصل على الفايروول ... ما هي المنافذ المفتوحة والمغلقة وماذا يحصل ... وهو موجود مع نظام سوزي ... لا أعلم إن كان موجود مع توزيعة أخرى ...

3- ملف الـ lastlog

ويتم تسجيل فيه من المستخدمين الذين لديك ومن فيهم قام بالدخول على النظام ومتى دخل عليه ... كل هذه الأمور مسجلة فيه ... ولأن هذا الملف هو ليس عبارة عن ملف ASCII عادي بل هو عبارة عن Binary هههههه أنا ... مجرد مزحة ... وبما إنه نوعه Binary إذن لا يمكن فتحه مثل الملفات الأخرى بأدوات العادية لكن يجب عرضه من خلال الأمر lastlog ... أكيد سيسأل سائل ... لماذا أقول لكي يصعب التعديل على من الذي دخل على الموضوع من خلال تحريره بأي محرر ... إذن Binary فوائده كثيرة هههههههههه ...

4- ملف الـ mail

هذا الملف يتم تسجيل الأمور التي يقوم نظام الميل mail على جهازك ... جميع الأمور المتعلقة بالميل تسجل هنا ... سواءا إرسال إستقبال كلها هنا أو في ملحقاتها ... مثل mail.err الي يسجل فيه الأخطاء وهكذا ...

5- ملف الـ wtmp

يتم تسجيل فيه كل مستخدم متى قام بالدخول الى النظام ومتى خرج ... ومن أين دخل على النظام وما هي المدة التي أستغرقها داخل النظام ... ولأنه الملف أيضا ليس نوعه ASCII TEXT فلذلك يجب أن تعرض محتواه من خلال الأمر التالي: last

6- ملف الـ messages

هذا هو اهم ملف تقريبا في النظام ... لأنه أغلب الأحداث تسجل فيه ... تشغيل خدمات ... خدمات فيها مشاكل لا تعمل ... الحصول على IP ... الأفعال التي يقوم بها المستخدم على النظام ... الأفعال التي يقوم بها النظام نفسه ... في تشغيل خدمات معينة ... في غلقها ... في كل شيء تقريبا تجدها هنا ... طبعا هذا الملف هو مجرد ASCII TEXT ولهذا ممكن تعرضه في أي برنامج للعرض التي سأذكرهم لاحقا ...

للمن لديه خبرة في هذا الملف ... فهو من أكثر الملفات التي تحبها الأداة Guru-Antilog حق أخونا sAFA7_eLNeT الشهيرة ... تجدها هنا ...

نأتي الى المجلدات:

1- مجلد الـ YaST2
وفيه يتم تسجيل جميع الأمور التي تحصل من خلال الأداة yast ... كل ما تعمله الأداة مسجل هنا ...

2- مجلد الـ cups
وفيه يتم تسجيل جميع الأمور التي تخص تعريف الطابعات والطباعة لديك ... سواءا على شبكة أو كانت مربوطة مباشرة كلها تسجل هنا ... فهي المكان الرئيسي لتسجيل جميع الأفعال التي تحصل مع الخدمة cupsd.

3- مجلد الـ samba
هنا يتم تسجيل جميع الأفعال التي تحصل مع الخدمة السامبا ... التي تستعمل في مشاركة الملفات بين انظمة التشغيل وغيرها من الأمور الكثيرة التي تقدمها هذه الخدمة ... كل ما يخصها تجده هنا ...

4- مجلد الـ squid
هذا المجلد يتم تسجيل فيه جميع الأفعال التي تقوم بها خدمة الـ squid ... فيها عدة ملفات ... منها لتسجيل الأخطاء ومنها لتسجيل المواقع التي يتم زيارتها من قبل المستخدمين على الشبكة المربوطة بسيرفر الـ squid ... وأيضا الكثير من الأمور الأخرى ... بإمكانك الدخول اليه والتفرج بنفسك ...

خامسا: ما هي أهم أدوات عرض اللوج ؟

كما أتضح لنا في الأعلى إنه البعض منها لا يمكن عرضه من خلال أدوات التصفح العادية وتحتاج الى أدوات

خاصة مثل الـ last والـ lastlog ... أما الملفات الأخرى فيمكنك عرضها من خلال التالي:

1- الأمر less ويمكنك إستعماله كما يلي:

```
less /var/log/messages
```

2- الأمر more ويمكنك إستعماله بنفس الطريقة التي مع الأمر less

```
more /var/log/messages
```

3- الأمر الذي هو جدا مهم وهو tail ... هذا الأمر يقوم بعرض آخر ملف معيين ... وفي حالتنا سنحدد له أن يعرض آخر ملف اللوج وهذا ما نحتاجه غالبا بالضبط ... خاصة لما تريد تشغل خدمة معينة مثلا الـ httpd ... وتظهر لك مشاكل ... وتريد تقرأ آخر اللوج لأنه أكيد المشكلة في الاخير تم تدوينها لأنها حصلت الحين ... وقتها ننفذ التالي:

```
tail /var/log/messages
```

الآن هذا بصفة أساسية سيعرض لك فقط آخر 10 سطور ... لماذا لا نجلعه يعرض آخر 25 سطر ؟ إذن نعمل التالي:

```
tail -n25 /var/log/messages
```

طيب الحين لنفرض نريد أن نراقب هذا الملف بصورة Live أو كل شي يحصل في الـ run time نراه في نفس اللحظة نعمل ماذا ؟ أعمل التالي:

```
tail -f /var/log/messages
```

تحب تزيد عدد السطور فقط أضف الـ n25- على الأمر وسيعرض لك 25 سطر، ماذا لو 50 سطر ؟ هههه

سادسا: كيف نقرأ محتوى أحد ملفات الـ Log ؟

أوكي هذا صراحة السؤال ليس سهلا وليس صعبا ... ولكن غالبا أصحاب الخلفية البرمجية يمكنهم فهم المحتوى بسهولة وذلك لأنه المحتوى أيضا عبارة عن أكواد ... لكن أكواد لم تكتبها أن بل كتبها لك النظام ولهذا فهي مفهومة لهم ... لكن هذا لا يعني إنه الذين ليس لديهم خلفية برمجية لن يفهموا منه شيئا ... لا بالعكس أيضا يمكنهم فهم ذلك كل ما عليهم هو المتابعة معي ... وطبعا المبرمجين تابعوا معي أيضا ...

لنفرض قمنابالتالي:

```
binary:/var/log # tail /var/log/messages
Dec 25 14:10:04 binary dhclient: DHCPREQUEST on eth0 to 10.0.0.1 port
67
Dec 25 14:10:04 binary dhclient: DHCPACK from 10.0.0.1
Dec 25 14:10:04 binary dhclient: bound to 10.0.0.4 -- renewal in 1483
seconds
```

.

الآن لنأتي لنفصل كل ما في هذه السطور ...

السطر الأول:

أولا ماذا تعني Dec 25 14:10:04 ؟ تعني التاريخ الذي بدأت فيه العملية ...

ثانيا ماذا يعني binary ؟ هذا هو أسم الجهاز على الشبكة أي الـ Hostname ...

ثالثا dhclient ما هي ؟ هذه خدمة service موجودة على النظام تقوم بعملية طلب الـ IP من الـ DHCP Server لكي يقوم بتثبيته على الجهاز ...

رابعا DHCPREQUEST هذه هي نوع الـ packet المرسلة من قبل dhclient والتي تطلب فيها IP من الـ DHCP Server الموجودة على الشبكة ...

خامسا on eth0 تعني العملية تمت على كارت الشبكة الي أسمه eth0

سادسا to 10.0.0.1 هي الجهة التي تم إرسال الـ packet من برنامج dhclient اليه من خلال المنفذ eth0

سابعا port 67 أي بإستعمال المنفذ port هذا ...

فالنعيد مرة ثانية ما شرحناه ... السطر الأول يعني إرسال packet من نوع DHCPREQUEST من خلال كارت الشبكة eth0 الى الجهاز الي رقم الـ IP له 10.0.0.1 من خلال المنفذ port 67 في الساعة 14:10:04 في اليوم 25 من شهر 12 ... هل هذا صعب ؟ لا أعتقد ذلك ...

السطر الثاني:

سأبدأه من عند DHCPACK وذلك لأنه جميع ما سبق هو نفس الي في السطر الذي سبقه ... طيب الـ DHCPACK ما هي ؟ هي نوع من أنواع الـ packets التي يرجعها الـ DHCP Server الى البرنامج dhclient ... أما from 10.0.0.1 فتعني إنه الـ packet هذه جاءت من الجهاز الذي يحمل هذا الـ IP

السطر الثالث:

أيضا bound to 10.0.0.4 تعني تم ربط جهازك بالـ IP الذي رجعه لك الـ DHCP Server والذي هو 10.0.0.4 ... والعبارة هذه -- renewal in 1483 seconds. تعني إنه سيرجع يطلب IP بعد 1483 من الثواني ... والذي هو تقريبا 25 دقيقة ...

هل هناك مشكلة الحين في قراءة ملف أو Log معيين ؟ أكيد المسألة ستختلف من ملف الى آخر ... وذلك لأنه المحتوى سيكون حسب ما خصص ذلك الملف له ... ومسألة شرح جميع السطور في كل الملفات وأشكالها صعب جدا ويمكن تأخذ منا شهور لكثرتها وكثرت ما تحتويه .... لكن أفهم كيف يبنى ملف الـ Log بغض النظر عن نوعه فكلمه تابعين للقاعدة التالية:

1- يبدأ بتاريخ ووقت التنفيذ

2- أسم الجهاز hostname الذي تم الدخول اليه أو بعض المرات أسم عام للخدمة التي طلبت التنفيذ مثل: linux kernel والتي تعني إنه الكيرنل هو من قام بها ... وبعض الملفات ممكن يكون أسم المستخدم ... تختلف حسب نوع التدوينه ...

3- الخدمة التي قامت بالعمل أو بتنفيذ شيء معيين ...

4- نوع الحدث الذي تم ... إرسال بيانات ... تنفيذ أو تشغيل خدمة معينة مثلا:

```
binary:/var/log # /etc/init.d/named start
Starting name server BIND
Warning: File, /etc/named.conf.include not found.  Creating it.
done
```

حيث قمت بتشغيل خدمة الـ named والتي هي الـ DNS ... وقال لي إنها أشتغلت تمام وقامت بإنشاء الملف

```
/etc/named.conf.include
```

من تلقاء نفسها لعدم وجوده بالسابق ... الآن لنفتح آخر الـ Log لنرى ماذا كتب هناك ... نرى كالتالي:

```
Dec 25 23:33:57 binary named[15638]: starting BIND 9.3.2
-t /var/lib/named -u named
Dec 25 23:33:57 binary named[15638]: found 1 CPU, using 1 worker
thread
Dec 25 23:33:57 binary named[15638]: loading configuration from
'/etc/named.conf'
Dec 25 23:33:57 binary named[15638]: listening on IPv6 interfaces, port 53
Dec 25 23:33:57 binary named[15638]: listening on IPv4 interface lo,
127.0.0.1#53
Dec 25 23:33:57 binary named[15638]: listening on IPv4 interface eth0,
10.0.0.4#53
Dec 25 23:33:57 binary named[15638]: command channel listening on
127.0.0.1#953
Dec 25 23:33:57 binary named[15638]: command channel listening on ::
1#953
Dec 25 23:33:57 binary named[15638]: zone 0.0.127.in-addr.arpa/IN:
loaded serial 42
Dec 25 23:33:57 binary named[15638]: zone localhost/IN: loaded serial 42
Dec 25 23:33:57 binary named[15638]: running
```

طبعا يخبرني إنه تم عملية التشغل للخدمة وقام بتحميل الإعدادات من ملف

/etc/named.conf

وحاليا يتصنت على كل من الشبكة الداخلة lo والشبكة من خلال eth0 ... وإنه قام بتشغيل الزون للـ local domain ... وبالختام أخبرني إنه كل شي يعمل الحين من خلال كلمة running

5- العمل الذي قامت به الخدمة المذكورة ... والذي يكون بعد الرمز ":" ...

في الختام الموضوع صراحة طويل طويل جدا ... وصعب أن أقوم بتغطيته لوحدي ... ولهذا أتمنى لو يشارك الجميع في إكمال هذه الدليل الذي سيكون إن شاء الله مرجع جيد للعرب في التعامل مع ملفات الـ Log ... الموجودة على جهازك والتي تسهل عليك الكثير من الأمور ... خاصة عند حصول مشكلة عندك على الجهاز ... أو في حالات الإختراق والأمور الخاصة بالحماية ... كلها تكون مسجلة في الـ Log إلا إذا تدخل برنامج مثل برنامج أخونه سفاح وقام بحذف هذه الملفات ... هنا أقول لك هناك حل آخر وهو أنك تعمل التسجيل يكون remotely أي على سيرفر خارجي ... وليس على نفس السيرفر أو الجهاز الذي نتكلم عليه ... مجرد معرفتك لأنواع ملفات تسجيل الـ log ستسهل عليك أين تبحث وبعد ذلك قمت بشرح أنا كيف تبحث وكيف تقرأ المحتوى ... أرجوا أن يكون الموضوع قد نال على رضاكم ...

أخوكم B!n@ry ...