Linux Security Policy HowTo

السلام عليكم ورحمة الله وبركاته ..

مراحل تطبيق الحمايه ..

1) Physical Security
كثيرا من مدراء السيرفرات لا يعيرون اهميه بالغه لهذا النوع من الحمايه ولهذا غالبا ما يقعون في مشاكل كثيره سأتناول بعض منها من واقع محلي والبعض الاخر من الدراسه والبحث اول امر هو غرفة السيرفر هل هو محمي ام لا ؟ بمعنى هل هناك ضوابط لدخوله ام هي مجرد يدخلها الرايح والجاي بالمصطلح العامي .. ثانيا هل السيرفر يقع في بيئه مناسبه له للعمل لساعات طويله ؟ اي يجب وضعه في غرفه ذات درجة حراره تسمح له بالعمل دون توقف إن ارتفاع درجة حرارة الغرفه يؤدي الى وقف عمل السيرفر سواءا ذاتيا او قسريا ولذلك ينصح ان تكون الغرفه تحت درجة حرارة 16-17 درجة مئويه ..
وايضا مسأله اخرى وهي الخادم الاحتياطي ويفضل ان يكون هناك خادم في مكان خارجي ... يعني يفضل تكون مجهز امورك لاي مشكله قد تطري على الخادم الرئيسي مما يؤدي الى وقف العمل ..

طبعا كل هذا يعتمد على طبيعة واهمية العمل الذي لديك من هذه الامور والمشاكل التي قد تحدث الكوارث الطبيعيه كالحرائق والفياضانات وايضا مشاكل قطع العتاد hardware وغيرها

كل ما يتم ذكره يعتبر اقتراق لامن الخادم والمعلومات التي عليه .. اي تلف او توقف يعتبر بحد ذاته تقصير في الامن والتي تقع ظمن مفهوم التقصير في ال availability ايضا وقبل ان انسى امرا مهما في physical sec وهو الحمايه على مستوى ال BIOS ووضع كلمات سريه للوصول الى اي اداتها وايضا وضع كلمات سريه على ال BOOT loeder لكي لا تسمح للاخرين من تمرير خيارات معينه الى ال kernel

2) User Security
هنا ايضا مسأله يغفل عنها الكثيرون بحيث يتم استعمال المستخدم root لتنفيذ جميع العمليات ومن جميع المدراء الموجودين في الشركه مثلا ...
يعني لو نفرض لدينا 3 مدراء admin في مؤسسه واحد للشبه وآخر لقواعد البيانات والثالث هو الرئيس مثلا ..
الحين قام احدهم باستخدام المستخدم root لتنفيذ مسأله معينه وادت الى توقف عمل الخادم .. كيف نعرف من هو المسؤول من هؤلاء الثلاثه ؟ ستقول لي من ال log file اقول مضبوط عرفت المستخدم على الجهاز لكنك لم تعرف من هو ال admin الذي استعمل هذا المستخدم root وحصلت المشكله بسببه لذلك يفضل عمل مستخدمين ويحصل كل مستخدم على صلاحيات ليؤدي وظيفته فقط .. يعني admin الشبكه له صلاحيات على اوامر الشبكه فقط وال admin الي على قواعد البيانات له صلاحيات على اوامر القواعد فقط .. وهكذا ..
يمكنك ان تعمل هذا من خلال الامر sudo مثلا الان ستسهل عليك مراقبة الجميع ومعرفة كل ماذا عمل .. لانه حصلت معي مره في احدى المسؤسسات كانوا admins يدخلون ويعملون من المستخدم root في نفس الوقت وكل واحد يخرب على عمل الثاني دون قصد ..

File & Filesystem Security (3

عند الحديث عن الحمايه على مستوى ال fs فانه يجب علينا ان نكون مدركين لنوعية البيانات التي ستوضع عليه وايضا ماهي الخيارات المستعمله لل mount عليه نأتي لنوضح اكثر .. البيانات هي هي مهم جدا ؟
ان كان الجواب نعم ممكن استعمال خواص التشفير ليقوم بتشفير جميع ما يكتب على هذا ال fs لكن يجب ان تأخذ بنظر الاعتبار الكفاءة والسرعة في القراءة والكتابة ولن تكون عالية بسبب مسألة تشفير البيانات عند الكتابه وفك تشفيرها عند القراءة في هذا ال fs .. اما الخيارات المستعمله لعملية ال mount ايضا يجب ان يكون اختيارها بدقه يعني لنفرض لديك ملفات لا تريد مشاركتها داخل مؤسسه او جامعه ولا تريد ان يتم التلاعب بها من اي شخص فبالتأكيد ستقوم بوضع خيار ro بدل من rw على هذا ال fs . ايضا مسأله اخرى بالنسبه لل mount و umount لهذا ال fs وغيرها من الامور المهمه ينصح بمراجعة man mount و man fs

بالنسبه للحمايه على مستوى الملفات فهناك ثلاث مستويات :
1) المستوى الاول وهو المستوى الذي تكون فيه الحمايه عاليه جدا بحيث تسمح لل ownerبان ياخذ من صلاحيات مطلقه وان لا تعطي صلاحيات اخرى لاي شخص
2) المستوى الثاني وتكون الحمايه فيه متوسطه وهذا هو المستوى الاساسي في اغلب الانظمه حيث يكون للمالك owner كامل الصلاحيات وللاعضاء في نفس المجموعه القراءة والتنفيذ وكذلك بالنسبه للمستخدمين الآخرين الذين هم ليسوا المالكين ولا يقعون ظمن نفس مجموعة المالك
3) المستوى الثالث والذي يكون اضعف بكثير مما سبق بحيث يكون للجميع حق القراءة والكتابة والتنفيذ
يمكنك الانتقال من مستوى الى آخر من خلال umask ولكن عليك ان تختاره بصوره جيده لكي لا يقع في مشاكل لاحقا ..

هناك امور اخرى على مستوى الملفات بحيث في الانظمه الحديثه مثل ext3 تم اضافة محكمات اخرى على مستوى الملف والتي تسمى attributes بحيث يمكنك استعمالها ايضا لغرض زيادة الحمايه مثلا

```
chattr    +i    file
```

هذه ستضيف خاصيه اسمها immutable بحيث تمنع اي شخص من حذف او الكتابه على الملف نهائيا الا لو قمت برفع الخيار هذا عنه .. ويوجد خيارات اخرى كثيره لا مجال لحصرها هنا ايضا قبل ان انسى يجب ان تراعي ال stickybit وال setGUID وال SUID بحيث تراعي اين ستقوم بوضعها ؟ وما هي البرامج مثلا التي سوف تمتلك صلاحيات SUDI ؟ هذه امور مهمه جدا من خلالها بامكانك زيادة قوة الحمايه لديك ايضا يفضل استعمال Integrity checker لكي تتاكد من سلامة البرامج binaries التي لديك لانه ممكن يكون برنامج مثلا mount لديك يقوم بوظائف اخرى غير المخصص لها .. طبعا هذه البرامج التي تساعدك هي tripwire وعلى حد علمي لم يعد مجاني مثل الاول لذلك ابحث عن برنامج opentripewire في sourceforge سيقوم هذا البرنامج بمقارنة ملفاتك مع ملفات موجوده في قاعدة البيانات يتم المقارنه معها للتأكد من صحة هذه البرامج التي لديك ...

قبل ان نختم هذا الجزء احب التنويه الى حصان طرواده trojan horse حيث ممكن يكون المخترق قام بتوزيع برنامج معين على النت ويطلب استعماله وتنفيذه باستخدام صلاحيات root لكن فعليا هو ينفذ امور اخرى في الخفاء او الظهر ستقول لي كيف اكتشف ذلك ؟ اقول لك ابسط الطرق هي استعمال تواقيع ال MDS checksum وال GPG التي تاتي مع ال rpm التي ستقوم بتنصيبها يعني بعباره اخرى لا تنزل برنامج على سيرفر مهم دون التاكد من التوقيع الخاص بهذا البرنامج ...

Password Security & Encryption (4

هذا الجزء متشعب وكبير جدا نظرا للتقنيات الكثيره المتوفره على النت ولهذا ساحاول الاختصار قدر الامكان

اولا .. لو كان لديك معلومات ممه يتم ارسالها من خلال الشبكات المفتوحه Public Network والذي هنا نقصد به الانترنت استعمل PGP وال Public Key Eneryption في التشفير .. وان كان ما ترسله على النت مهم جدا كأن يكون اموال الكترونيه اطلب توقيع من شركة وسيطه بحيث توقع على ال public key الخاص بك وال public key الخاص بالطرف الاخر وهي ستكون Main Authority بينكم مثال على هذه الشركات Verisign

ثانيا .. استعمل ال ssl وال https لزيادة الحمايه على الاتصالات الي تطلب verification مثلا للدخول الى حساب بنكي ومن هذه الامور ويفضل ان تقوم بربطهم مع شركة ثالثه الوسيط كما ذكرنا في الاعلى وايضا استعمال MIME type التي لا تفرض بعض الصغرات او تكون هي بحد ذاتها ثغره امنيه عليك .. وايضا لا تستعمل MIME type غير معروف وغير تابع الى standard معينه لانه سيجلب لك نفس المشكلة التي ذكرتها ..

ثالثا .. استعمل secure shell في الاتصال بالسيرفر من مكان آخر remotely .. حيث يمكنك من خلال ال ssh ان توفر قناه امنيه الى حد كبير جدا عند اتصالك بالسيرفر .. وايضا يمكنك التحديد من مسموح المرور ومن لا من خلال التوقيع المستعمل Signiture
رابعا .. استعمال ال PAM الي تمثل .. Pluggable Authentication Modules حيث يمكنك التحكم بالكثير من وسائل الحماية على السيرفر من خلال هذه ال Modules ايضا عند تطوير نظام معين او برنامج لا حاجة لك لتطوير وسائل حماية له لانك ممكن ان تشغل له وسائل حمايه من خلال PAM

Kernel Security (5

يعتبر الكيرنل من الامور المهمه التي يجب ان تنتبه لها من حيث الامن لانه ما فائدة نظام محمي بشكل كبير لكن الكيرنل المستعمل فيه مشاكل وثغرات ؟؟ وكما تعلمون الكيرنل اساس لينوكس ولهذا هو مهم جدا ان يكون على درجه عاليه من الحمايه .. تخيل بناء جميل جدا ولكن اساس هذا البناء هش .. ؟ اكيد سينهار في لحظه معينه .. هذه اللحظه في لينوكس خطيره جدا لانه اذا استطاعوا ايقاف الكيرنل فذلك يعني انهيار النظام بالكامل ..

الخطوات المتبعه لتقوية حماية الكيرنل لديك وبالتاكيد النظام هي :
1) تحديث الكيرنل من فتره الى اخرى لانه 90 % من التحديثات التي تطرأ على الكيرنل هي تحديثات امنيه
2) تشغيل الجدار الناري Firewall وإعداده بشكل صحيح لكي يقوم بالتصدي للهجمات الموجهة على ال Box
3) إعداد خيارات الكيرنل بشكل جيد ومدروس من خلال sysctle .conf مثال على ذلك عمل ايقاف لل ping على السيرفر من خلال

```
echo "1" >  /proc/sys/net/ipv4/icmp-ignore-all
```

او تشغيل tcp-syn****ies لمنع الهجمات من نوع DOS الذي يستهلك المصادر التي لديك مما يجبر الكيرنل لعمل اعادة تشغيل للسيرفر لديك .. هناك الكثير من الخيارات الأخرى التي ممكن تعمل لها اعداد على مستوى الكيرنل ..... لمزيد من المعلومات راجع google ...

مسأله اخيره احب ذكرها عندما نتحدث عن الحمايه على مستوى الكيرنل هو Kernel Devices نعم هما جهازان

```
dev/urandome/
```

و

```
dev/random/
```

حيث توفر هذه الاجهرزه Random Number's في اي وقت تطلب منها ذلك ... يتم استعمالهما عند عمل مفاتيح من نوع PGP keys او تواقيع الخاصه بال ssh وغيرها الكثير من البرامج ...

هذا ما لدي على مستوى الكيرنل وانا متاكد ان هناك المزيد لكن عليكم بال .. Google ...

Network Security (6

اعتقد ان هذا من اكبر الجوانب الامنيه التي يصعب علي حصرها لكم .. لكن سأحوال جاهدا ان اذكر لكم اهم الامور فيه والتوسع متروك لكم .. على بركة الله ..

اولا .. تشغيل الجدار النار لديك بشكل ممتاز من خلال iptables ويمكن الرجوع الى شرح الاخ sAFA7_eLNeT في هذا الامر على الرابط التاليه هنا

ثانيا .. تشغيل ال tcp-wrappers وعمل امداد لها بصوره جيده بحيث تطبق قاعدة معينة اما انك تسمع للكل وتمنع البعض او انك تمنع الكل وتسمح للبعض من خلال ملفات

```
etc/hosts.deny/
```

او

```
etc/hosts.allow/
```

طبعا هناك الكثير من الخدمات التي يمكن التحكم بها من هذه النقطه مثلها ال FFp وال ssh وال pop3 وغيرها ... وأيضا هناك شرح للأخ sAFA7_eLNeT له هنا

ثالثا .. عمل الحمايه اللازمه على ال DNS التي لديك بحيث لا تسمح لجهاز خارجي من تسجيل نفسه على ال DNS الذي لديك ...

رابعا .. عمل الحمايه اللازمة على مستوى ال MTA والي هو (Mail Transport Agent) بحيث لا تسمح للناس بعمل overlog من سيرفرك وبالتالي ينتج مشاكل السبام الخارجه منه ...

خامسا .. عمل حمايه على مستوى ال Network file system الي هو NFS .. بحيث تعمل الحمايه اللازمه لكي يتم عمل mount فقط للاشخاص المصرح لهم بذلك والبقيه لا .. للمزيد راجع NFSHowTo ...

سادسا .. عمل حماية على نظام Network Information Service الي هو NIS والذي كان يسمى YP من كلمة Yallow Pages بحيث لا يتم كشف المعلومات التي يقدمها هذا النظام للعالم الخارجي سوى لمن هم مصرحين بذلك .. لانك كما تعلم هذا النظام عمل تصاريح الدهول الكاملة للسيرفر

ان كان موجود ولذلك السيطرة عليه معناه كارثه .. طبعا لم يعد NIS محمي كثيرا مثل السابق لذلك يفضل استعمال LDAP بدلا منه ..

سابعا .. استعمل برامج مهمه لكشف العيوب التي لديك .. مثلا نضرب مثال :
قمت بتعيين ports لخدمات معينه كيف ستجربها ؟ استعمل برنامج مثل nmap لشكف ما خي ال ports المفتوحه وماهي المغلقه على سيرفرك ... ويوجد الكثير من البرامج لكن بالنسبة لي هذا هو البرنامج رقم واحد .. ما ذكرناه هو لمراقبة المنافذ ports الحين لكي تقوم بمراقبة وتحليل الشبكه لديك وماهي البرامج الخارجه وما هي الداخله على جهازك استعمل برامج التحليل packets او ما يسمى بالـــ sniffers ... منها dsniff و ethreal وتفرج على المعلومات التي تدخل وتخرج من سيرفرك ... لتقرأ أكثر على ال sniffers أيضا الأخ sAFA7_eLNeT الله يجزيه الخير له موضوع في ذلك هنا
نقطه صحيح تذكرتها الحين ... لا تقوم انت بعمل فحص المنافذ port scanning التي على سيرفرك من داخله .. بل اطلب من صديق او اعملها انت من مكان خارجي .. ! ! لا تسألني لماذا .. أكتشف هذه المسأله انت بنفسك ...

اعتقد كما ذكرت لكم مهما كتبت هنا فلم اكتب بالحقيقه شيء لكن ممكن يكون ما كتبته محل فائده للبعض وعدم الفائدة للاخرين ..

Before Going Public (7
الى حد الآن قمنا بالكثير من التحضيرات والفحوصات لكي نذهب Online ... لكن هناك نقاط مهمه يفضل النظر اليها قبل ان تجعل سيرفرك مشبوك الى العالم الخارجي Plugged to the outworld وهي كالتالي :
1) اختيار خطة مناسبة لعمل ال Backup وهذه صراحه متغيره من خدمه الى اخرى لهذا صعب احصائها هنا لكن الاضرار فيها ذكر مثال على ما اقصد .. يعني لنفرض لديك شركة تقدم خدمات بنكية .. هنا يفضل يكون الفتره التي يتم اخذ النسخه الاحتياطيه Backup قليله جدا لكثرة التغيرات المهمه التي تحصل على رصيد العميل ... وطبعا هذا على حساب الاداء والمساحه لذلك انتبه الى ذلك ..

2) اوكي أخذت باك اب وصار عندك مشكلة اتيت ترجع الباك اب وجدته فيه مشكله .. هنا كارثه ولهذا ينصح تجربته قبل ان تغيير نفسك لديك نسخه احتياطيه اصلا ..

3) عمل فحوصات دوريه على المستخدم لديك وعلى ملفات ال log الخاصه بالسيرفر والخدمات التي عليه ويمكنك ان تعمل تقارير من هذه الفحوصات يتم ارسالها لك على البريد من خلال إعدادات الخاصه بال syslogd وايضا باستعمال ال crond

4) متابعة التحديثات الامنيه التي تصدر هي احدى اهم نقاط المهمه التي يجب متابعتها لانه كما تعلم مهما وصلت الى درجه من الحمايه العاليه فانه ممكن تصدر ثغره جديده انت لم تقوم بترقية الخدمة التي تنفذ عليها ويروح السيرفر عندك في داهيه .. .. .. طبعا ممكن تعمل برامج تتابع لك هذه الامور ولكن هذه من اختصاص السفاحين .. هههههههه

في الختام اتمنى ان ينال الموضوع رضاكم واعجابكم الموضوع مهدى لمجتمع لينوكس العربي بصوره عامه وللاخ amine00 بصوره خاصه وآخيرا وليس اخرا إن شاء الله مهما وصلت من قوة الحماية فلن تصل الى 100 % ولا حتى 99 % هذا رأيي المتواضع والعالم كله يخضع لقانون مهم جدا وهو "الكمال لله سبحانه وتعالى" ...

اخوكم .. ابو محمد ...