Quantar Solutions Ltd. – إدارة المخاطر التشغيلية للشبكات (nORM)
دليل تثبيت وتشغيل نظام المراقبة

الإصدار 2 – يناير 2009

1 مقدمة 1
2 تثبيت قاعدة البيانات وخادم الملفات 2
2.1 تثبيت النظام الأساسي 2
2.1.1 إرشادات تفصيلية 2
2.2 إنشاء مفتاح ssh المشترك 3
2.2.1 إرشادات تفصيلية 3
2.3 إعداد خادم NTP 3
2.3.1 إرشادات تفصيلية 3
2.4 إعداد خادم Samba + مستودع 3
2.4.1 إرشادات تفصيلية 3
2.5 تكوين قاعدة البيانات 4
2.5.1 إرشادات تفصيلية 4
2.6 إعداد Cron + تكوين createXML 4
2.7 دليل تكوين Snort + تحديث مدقق cron 4
2.7.1 إرشادات تفصيلية 4
2.8 ملف التعيين 5
3 تثبيت جهاز العرض 5
3.1 تثبيت النظام الأساسي 5
3.1.1 إرشادات تفصيلية 5
3.2 عميل NTP لخادم قاعدة البيانات 6
3.3 نسخ المفتاح العام من خادم قاعدة البيانات 6
3.4 تثبيت Snort 6
3.4.1 إرشادات تفصيلية 6
3.5 تكوين تزامن snort 6
3.6 تثبيت برمجة نصية لجهاز العرض 6
4 اعتبارات تشغيلية 7
4.1 ملف التعيينات 7
4.2 قواعد Snort 7
5 مرجع للوثائق الأخرى 7

1 مقدمة

يحدد هذا الدليل متطلبات التثبيت الخاصة بالجهازين اللازمين للمراقبة. الأقراص المضغوطة اللازمة للتثبيت هي:

- Ubuntu “Dapper” Server 6.06
- FreeBSD 6.1
- قرص مضغوط لبرامج إضافية يحتوي على:
  - برنامج نصي لتهيئة قاعدة بيانات MySQL Snort
  - برنامج نصي لإنشاء XML + مكتبة + نموذج ملف تعيين
  - دليل تكوين snort أولي (يتضمن تنبيه تحكم سلبي)

- تحديث البرنامج النصي لـ snort
- برنامج مراقبة نصي+ ملف تكوين

توضح الأقسام التالية تثبيت قاعدة البيانات وخادم الملفات ثم جهاز العرض.

سيتم استخدام عنوان IP 10.0.0.1 خلال هذا المستند للإشارة إلى خادم قاعدة البيانات و10.0.0.2 الخاص بجهاز العرض. قم باستبدال هذه البيانات كما هو مطلوب.

نظرًا لأنه يلزم تكوين البرامج النصية، راجع البرنامج النصي المفرد الخاص بالإرشادات.

2 تثبيت قاعدة البيانات وخادم الملفات

للحصول على معلومات إضافية، بخلاف هذا الدليل، راجع:

http://help.ubuntu.com/6.06/ubuntu.serverguide/C/index.html

2.1 تثبيت النظام الأساسي

قم بتثبيت خادم LAMP الأساسي من قرص Ubuntu Dapper 6.06.

متطلبات خاصة:

- تحتاج إلى تكوين منفذين للشبكة
  - عنوان إدارة خارجي
  - عنوان IP محلي على سبيل المثال 10.0.0.1 (للاتصال بجهاز العرض)
- المتطلبات الإضافية للحزمة
  - خادم-openssh (خاص بالإدارة عن بعد)
  - libhtml-parser-perl (لإنشاء XML)
  - libdate-simple-perl (للعمليات الحسابية الخاصة بالتاريخ)

لتثبيت حزم أخرى، راجع الأقسام المفردة أدناه.

2.1.1 إرشادات تفصيلية

1. قم بتشغيل الجهاز وأدخل القرص المضغوط (تأكد من أن الجهاز قد تم إعداده للتشغيل من القرص المضغوط).
2. عند الوصول إلى قائمة تثبيت Ubuntu، اختر "تثبيت خادم LAMP".
3. اختر اللغة المطلوبة وخيارات لوحة المفاتيح عندما يطلب منك ذلك.
4. عندئذ سيتم تثبيت المكونات الأساسية.
5. في حالة وجود خادم DHCP متوفر، سيتم تكوين منفذ الإدارة تلقائيًا. وإلا، قم بتكوين الشبكة يدويًا في النماذج المتوفرة.
6. عند المطالبة، قم باختيار نسخة متطابقة مناسبة من أرشيف Ubuntu (وقم بإعطاء وكيل HTTP معلومات إذا اقتضى الأمر).
7. حدد خيارات تقسيم القرص المطلوب؛ مع اختيار مسح القرص كله وينبغي أن يؤدي قبول التقسيم الافتراضي إلى استخدام القرص بأكمله في قسم واحد باستثناء التبديل.
8. قم بتعيين الساعة لـ UTC.
9. اختر اسم المستخدم وكلمة المرور المناسبة.
10. عندئذ سيتم تثبيت النظام الأساسي (قد يستغرق ذلك بعض الوقت).
11. عند الانتهاء من التثبيت، قم بإعادة التشغيل وإزالة القرص المضغوط.
12. بعد إعادة التشغيل، قم بتسجيل الدخول وتحديد خيار إزالة القرص المضغوط من قائمة /etc/apt/sources (مثل التعليق على سطر 'deb cdrom:...') وعدم التعليق على أي مصادر أخرى تم التعليق عليها.
13. قم بتشغيل: sudo aptitude update && sudo aptitude dist-upgrade لتحديث النظام.
14. قم بتثبيت الحزم الإضافية المطلوبة باستخدام:
    sudo aptitude install openssh-server libhtml-parser-perl libdate-simple-perl
15. قم في النهاية بإضافة، تكوين الشبكة الثانية في /etc/network/interfaces

2.2 إنشاء مفتاح ssh المشترك

إنشاء زوج من مفاتيح ssh بدون كلمة مرور، للمزامنة التلقائية بين الخوادم.

2.2.1 إرشادات تفصيلية

قم بتشغيل الأمر التالي:

ssh-keygen -t dsa

(استخدام أسماء الملف الافتراضية وعدم وجود كلمة مرور)

سوف يتم نسخ المفتاح العام إلى جهاز العرض لاحقًا.

2.3 إعداد خادم NTP

قم بإعداد خادم NTP للحفاظ على تحديث الوقت الخاص بجهاز العرض.

2.3.1 إرشادات تفصيلية

تثبيت خادم NTP:

sudo aptitude install ntp-server

قم بتغيير الخادم الافتراضي في /etc/ntp.conf من ntp.ubuntu.com إذا لزم الأمر.

في حالة تغيير الخادم (أو أي إعدادات أخرى)، قم بإعادة تشغيل NTP:

sudo/etc/init.d/ntp-server restart

2.4 إعداد خادم Samba + مستودع

إنشاء دليل لتخزين ملفات XML فيه.

قم بتثبيت خادم Samba لإثبات الوصول إلى الدليل.

2.4.1 إرشادات تفصيلية

في البداية قم بإنشاء دليل لملفات XML:

mkdir /mypath/xmlfiles

ثم قم بتثبيت Samba:

sudo aptitude install samba

قم بإنشاء كلمة مرور خاصة بالمستخدم الحالي:

smbpasswd

قم بتحرير ملف التكوين /etc/samba/smb.conf لتغيير مجموعة العمل إلى المجموعة المطلوبة، مع التأكد من أن المستخدم غير موجود في القائمة غير الصحيحة، وإضافة النقطة المشتركة، على سبيل المثال:

```
[share]
path = /mypath/xmlfiles
comment = shared xml files
browseable = yes
writable = no
```

قم بالتعليق على أي تعريفات مشاركة أخرى.

في النهاية، قم بإعادة تشغيل Samba:

sudo /etc/init.d/samba restart

2.5 تكوين قاعدة البيانات

إعداد قاعدة البيانات:

- قم بإضافة الوصول عن بعد للاتصال من جهاز العرض
- قم بإنشاء مستخدم snort
- قم بإنشاء قاعدة بيانات snort وبنية استيراد
- قم بمنح الأذون لمستخدم snort في قاعدة البيانات

2.5.1 إرشادات تفصيلية

قم بتحرير ملف تكوين MySQL /etc/mysql/my.cnf وإزالة السطر:

bind-address = 127.0.0.1

أعد تشغيل MySQL:

sudo /etc/init.d/mysql restart

قم بتشغيل MySQL:

mysql

أدخل سلسلة الأوامر التالية:

create user snort identified by 'password'; (استبدال كلمة المرور)

create database snort;

use snort;

source /pathto/create_mysql (برنامج التمهيد النصي الموجود على القرص المضغوط)

grant all on snort.* to snort@localhost identified by 'password';

grant all on snort.* to snort@10.0.0.2 identified by 'password';

flush privileges;

2.6 إعداد Cron + تكوين createXML

قم بنسخ برنامج createXML.pl النصي وملف المكتبة من القرص المضغوط وحرر خيارات التكوين داخل البرنامج النصي. قم عندئذ بإضافة عنصر إلى cron، لتشغيل البرنامج النصي مرة في الأسبوع.

إرشادات تفصيلية

حرر crontab:

crontab -e

وقم بإضافة السطر التالي:

* * * * 1 cd createXMLpath && ./createXML.pl

يعمل هذا على تشغيل برنامج createXML.pl النصي من دليله المحلي كل يوم اثنين.

2.7 دليل تكوين Snort + تحديث cron للمدقق

قم بنسخ دليل تكوين snort من القرص المضغوط الذي يتم توفيره (وقم بتحرير خط مخرجات snort.conf، عند الضرورة)، قم أيضًا بنسخ البرنامج النصي update_snort.pl (وقم بتحرير الخيارات كما هو مطلوب). قم بإضافة سطر إلى crontab للتحقق من طلبات التحديثات وفقًا للفترة المطلوبة.

2.7.1 إرشادات تفصيلية

قم بتحرير ملف snortconf/snort.conf وتغيير السطر التالي كما هو مطلوب:

output database: alert, mysql, user=snort password=password dbname=snort host=10.0.0.1

حرر crontab:

crontab -e

قم بإضافة السطر التالي (مثال على الفحص كل ساعة):

0 * * * * cd updatesnortpath && ./update_snort.pl >/dev/null

2.8 ملف التعيينات

بالإضافة إلى ذلك، من الضروري إدخال التعيينات المطلوبة من تنبيهات snort لأنظمة الأهداف المحلية في ملف التعيينات. راجع العمليات أدناه.

3 تثبيت جهاز العرض

للحصول على معلومات إضافية، بخلاف هذا الدليل، راجع: http://www.freebsd.org/docs.html

ينبغي تكوين جهاز العرض بشكل مثالي لاستخدام RAID0 الخاص بمحركات الأقراص الثابتة (لتكبير سرعة كتابة القرص لالتقاط البيانات الصادرة إلى الشبكة) قبل بدء عملية التثبيت.

3.1 تثبيت النظام الأساسي

قم بتثبيت النظام الأساسي لـ FreeBSD 6.1 باستخدام Kern-developer مع خيار المنافذ.

المتطلبات الخاصة:

- 3 منافذ الشبكة:
  - منفذ نشط مع عدم وجود IP (Intel NIC)
  - اتصال محلي على سبيل المثال 10.0.0.2 (للاتصال مع قاعدة البيانات)
  - اتصال خارجي (للتثبيت – يمكن تعطيله بعد التثبيت الأولي)
- حزم إضافية:
  - bash-3.1.10-1 (أو مكافئها)
  - تغيير shell الافتراضي إلى bash، لمستخدم الجذر
  - السماح بوصول SSH باعتباره جذر

3.1.1 إرشادات تفصيلية

1. قم بتشغيل الجهاز وأدخل قرص تثبيت FreeBSD.
2. اختر "Boot FreeBSD [افتراضي]" عند الطلب.
3. يتم الكشف عن الأجهزة الخاصة بالكمبيوترات التالية تلقائيًا. قد يستغرق ذلك بعض الوقت.
4. اختر الإعدادات الإقليمية المناسبة، عند الطلب.
5. اختر تثبيت "Express" عند "قائمة sysinstall الرئيسية".
6. في قائمة تقسيم القرص، استخدم الإعدادات الافتراضية بالضغط على 'A' ثم 'Q' على كلا الصفحتين. قم أيضًا، بتحديد خيار "BootMgr" لتثبيت FreeBSD Boot Manager.
7. اختر التوزيع "kern-developer" واختر "yes" عند الطلب لتثبيت المنافذ.
8. في "Installation Media" حدد HTTP ثم اختر موقعًا مناسبًا.
9. قم بتكوين واجهة شبكة الإدارة؛ يُمكن أن يحدث ذلك تلقائيًا إذا كان DHCP متوفرًا.
10. سوف يستمر التثبيت الآن. قد يستغرق ذلك بعض الوقت، يتوقف ذلك على النطاق الترددي للشبكة ومواصفات الجهاز.
11. حدد الحزمة التالية: shells->bash_3.1.10-1 (أو مكافئها)
12. بعد إعطاء كلمة مرور الجذر، تحقق من الخيار sshd لتمكين الوصول عن بعد.
13. يكون التثبيت الأساسي قد اكتمل الآن. سيتم إعادة تشغيل الكمبيوتر. قم بإزالة القرص المضغوط.
14. بعد إعادة التشغيل، قم بتسجيل الدخول كجذر وقم بتغيير shell الافتراضي إلى
    bash: chsh -s /usr/local/bin/bash root
15. قم بتحرير /etc/ssh/sshd_config وإلغاء تعليق السطر #PermitRootLogin وقم بتغيير الخيار 'no' إلى 'yes'. ثم قم بإعادة تشغيل برنامج ssh الخفي: /etc/rc.d/sshd restart
16. في النهاية، قم بتكوين بطاقة المراقبة في /etc/rc.conf

3.2 عميل NTP لخادم قاعدة البيانات

لتكوين عميل NTP، قم بتحرير /etc/ntp.conf وضع الأسطر التالية:

server 10.0.0.1 primary

driftfile /var/db/ntp.drift

أعد تشغيل برنامج NTP الخفي:

/etc/rc.d/ntpd restart

في النهاية، قم بإضافة السطر التالي إلى /etc/rc.conf لضمان تشغيل NTP عند تشغيل الجهاز:

ntpd_enabled="YES"

3.3 نسخ المفتاح العام من خادم قاعدة البيانات

قم بنسخ المفتاح العام من خادم قاعدة البيانات على سبيل المثال:

- mkdir ~/.ssh
- scp user@10.0.0.1:~/.ssh/id_dsa.pub ~/.ssh/authorized_keys

3.4 تثبيت snort

تجميع snort من المنافذ مع دعم وتثبيت MySQL.

- قم إنشاء دليل دليل السجل /var/log/snort

3.4.1 إرشادات تفصيلية

1. قم بتعيين متغير بيئة http_proxy إذا لزم الأمر.
2. cd /usr/ports/security/snort
3. قم بإجراء (فحص لخيار MySQL، عند الطلب)
4. سيتم الآن تجميع Snort. قد يكون هناك العديد من الرسائل التي تشير إلى أنه لا يمكن العثور على المصادر؛ هذه ليست سوى مشكلة فشل عملية التجميع.
5. قم بإجراء تثبيت (لتثبيت بنية snort)
6. mkdir /var/log/snort

3.5 مزامنة تكوين snort

اكتب (الكل في سطر واحد):

- rsync -ave ssh --delete user@10.0.0.1:/pathto/snortconf/ /usr/local/etc/snort

3.6 تثبيت البرنامج النصي لجهاز العرض

قم بنسخ البرنامج النصي لجهاز العرض (gather.sh) من القرص المضغوط.

يمكن تشغيل البرنامج النصي يدويًا أو تثبيته على دليل rc.d ليتم تشغيله تلقائيًا عند تشغيل جهاز العرض.

4 اعتبارات تشغيلية

4.1 ملف التعيينات

هذا الملف عبارة عن ملف CSV بسيط بسطر واحد لكل تهديد. يحتوي كل سطر على خمس قيم:

- معرف الأمان SID – رقم التعريف الفريد الذي تم تعيينه لهذا التهديد بواسطة SNORT1
- تنبيه – يعتبر هذا اسم التهديد الذي تم توفيره بواسطة SNORT، ولكن يمكن تغييره بواسطة المسؤول.
- هدف – سمة Target كما هي مطلوبة بواسطة علامة تهديد nORM ويتم توفيرها يدويًا بواسطة المسؤول. القيمة الافتراضية "Unknown".
- فئة – سمة الفئة Category كما هي مطلوبة بواسطة علامة تهديد nORM ويتم توفيرها أيضًا بواسطة المسؤول. القيمة الافتراضية "Indiscriminate".
- الخطورة – هي سمة SeverityScore كما هي مطلوبة بواسطة علامة تهديد nORM. يتم حساب القيمة الافتراضية تلقائيًا من قيمة الأفضلية لـ SNORT. التعيين من SNORT إلى nORM هو $1 \rightarrow 10, 2 \rightarrow 7, 3 \rightarrow 4, 4 \rightarrow 1$.

لتحديد القيم المناسبة لهذا الملف، برجاء الرجوع إلى مستند تعيين الأهداف.

4.2 قواعد snort

لتحديث قواعد snort:

1. قم بتنزيل أحدث مجموعة قواعد من //www.snort.org/
2. قم بفك الملف
3. انسخ دليل القواعد إلى pathto/snortconf/ على جهاز قاعدة البيانات
4. قم بتنفيذ الأمر synchronisation من القسم 3.5

5 الإحالة إلى وثائق أخرى

انظر أيضًا مستند تعيين الأهداف (يناير 2009)