Snort (NIDS)

Author: Net Spider(Net_Spider@hackersclub.net)

مقدمة:

تعتبر أداة Snort من افضل الادوات التي تستخدم في انظمة كشف الاقتحام .. وهذا غير أنها من اداوت المصدر المفتوح .. وتعمل على العديد من المنصات .. ولكن يفضل استخدامها على انظمة Unix/Linux

في البداية سأقوم بتلخيص سريع عن عملية التثبيت في جهازي:
الاول ثبت pcre ودي تجيبها من http://www.pcre.org/
وتأكد من ان libpcap مثبته في نظامك .. وغالبا هاتكون موجوده .. لانها مهمه لاي سنيفر واكيد معظمكم
بيشتغل على سنيفرات
بعد مانزلت سورس Snort نفذت شوية الخطوات التالية:

كود:PHP
```
[root@zeus]# gunzip < snort-2.2.0.tar.gz | tar xfv -
[root@zeus]# cd snort-2.2.0
[root@zeus]# ./configure --prefix=/usr/local/snort \
                  --enable-smbalerts --enable-flexresp
                  --with-mysql --with-snmp --with-openssl
                   ; make ; make install
[root@zeus]# mkdir /usr/local/snort/etc
[root@zeus]# mkdir /usr/local/snort/rules
[root@zeus]# mkdir /var/log/snort
[root@zeus]# cp etc/ -R /usr/local/snort/etc
[root@zeus]# cp rules/ -R /usr/local/snort/rules
```

المهم بدون مانطول في موضوع التثبيت
عندنا ملفين مهمين /usr/local/snort/etc/classification.config :وده بيحتوي على معلومات مهمة عن تصنيفات الRules
والملف التاني وهو /usr/local/snort/etc/reference.config وده فيه لينكات ومواقع تعتبر كمرجع لل snortلما يكون فيه تحذير معين مثلا.

نبدء في تشغيل .. snort بالامر التالي

كود:PHP
```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort.conf
```

ولو ملف snort.conf موجود في مكان تاني غير مساره في الامر بكل بساطه
بعد ما شغلت الاداة وكل حاجه ماشية زي الفل .. اذا الاداة شافت محاولة هجوم او ما شابه فهتكون تحذير في ملف /var/log/snort/alerts

ممكن نجرب هل snort شغاله فعلا للتأكد اننا ثبتناها صح او فيه مشاكل
يعني بأختصار نعمل محاولة هجوم ونشوف ردة الفعل ... مثلا نعمل بنج على Brodcast للشبكة

كود:PHP
```
ping -n -r -b 217.139.12.255 -p "7569643d3028726f6f74290a" -c3
```

بالنسبة ل ٧٥٦٩٦٤٣ d3028726f6f74290aفهي تعني صلاحيات الروت او اي دي •

نروح نشوف في ملف .. /var/log/snort/alerts لو لئيت تحذير يبئى الاداه شغاله تمام
التحذير هيكون حاجه زي كده:

كود:PHP
```
10/10-05:32:10.464130  [**] [1:498:6] ATTACK-RESPONSES id check
returned root [**] [Classification: Potentially Bad Traffic]
[Priority: 2] {ICMP} 217.139.12.125 -> 217.139.12.255
```

بعد ماتأكدنا من عمل الاداة بشكل صحيح نبدء نتوسع في التعامل معاها

على فكرة snort في الوضع الافتراضي تعمل على كارت الشبكة .. eth0 فأذا عندك كرتين شبكة وتحب تشغلها على كرت غير الكرت الافتراضي ممكن .. كالاتي:

كود:PHP
```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort.conf -i eth1
```

والان لو تحبو تشغلو snort كأحد ال services في نظام ريدهات التي تكون تحت المسار
/etc/rc.d/init.d/لكي تسهل التعامل معها ولكي تستطيع تشغيل snort تلقائيا عن اعادة تشغيل
النظام
الاول انشأ الملف /etc/rc.d/init.d/snortd كالاتي

كود:PHP
```
touch /etc/rc.d/init.d/snortd
```

وضع به الكود التالي:
على فكرة الكود انا واخده من ملف /etc/rc.d/init.d/snortd الي يأتي مع snort على هيئة .. RPM بس
عدلت عليه بحيث يتناسب مع اعدادت التثبيت على جهازي اللي وضعتها في بداية الموضوع:

كود:PHP
```
#!/bin/sh
# snortd         Start/Stop the snort IDS daemon.
# chkconfig: 2345 40 60
# description:  snort is a lightweight network intrusion
# Source function library.
. /etc/rc.d/init.d/functions

# Specify your network interface here
INTERFACE=eth0

# See how we were called.
case "$1" in
  start)
     echo -n "Starting snort: "
        cd /var/log/snort
     daemon /usr/local/snort/bin/snort -A fast -b -l /var/log/snort -
D -i
     $INTERFACE -c /usr/local/snort/etc/snort.conf
     touch /var/lock/subsys/snort
     echo
     ;;
  stop)
     echo -n "Stopping snort: "
     killproc snort
     rm -f /var/lock/subsys/snort
```

```
    echo
    ;;
  restart)
    $0 stop
    $0 start
    ;;
  status)
    status snort
    ;;
  *)
    echo "Usage: $0 {start|stop|restart|status}"
    exit 1
esac

exit 0
```

بعد كده نفذ الاوامر التالية لكي يصبح الملف قابل للاستعمال معchkconfig

كود:PHP

```
chmod 775 /etc/rc.d/init.d/snortd
chkconfig --add snortd
chkconfig --level 345 snortd on
```

كده الاداة هاتشتغل في level 3 و ٥ اي عند اعادة التشغيل
وبأمكانك تشغل الاداة او عمل ريساترت لها بسهوله كالتالي

كود:PHP

```
service snortd restart
```

والان فرضا لو جهازك فيه كرتين شبكة ومثلا كل كرت متصل بشبكة غير الشبكة اللي متصل بيها الكرت الاخر .. ومحتاج تشغل snort على الكرتين في نفس الوقت والخرج لكل كرت يكون منفصل عن التاني ... ممكن تنفذها كالتالي:

كود:PHP

```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort.conf -i eth0
-l /var/log/snort0
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort.conf -i eth1
-l /var/log/snort1
```

طبعا بعد ماتكون انشأت مجلد /var/log/snort0 و/var/log/snort1

كل ده ولسه متكلمناش عن ال ,, Rules شكلنا هانأجله في موضوع تاني

المهم نكمل:
اداة Snort تعمل في وضعين اساسيين packet sniffer :وNIDS mode
في ال packet sniffer الاداة هاتشتغل ك سنيفر عادي بدون تحليل الباكت وتطبيق الرولز عليها
اما في NIDS mode فالاداة هاتشتغل ك نظام كشف اقتحام

تعالو نشتغل شوية في الpacket sniffer
لو حبينا نشغل Snort في الوضع ده فبكل بساطه هنطبق الامر التالي:

كود:PHP

```
/usr/local/snort/bin/snort -v
```

وهاتشوف ادامك على الشاشة الباكيت اللي ماشيه في الشبكة

لو حبينا نعرض معلومات عن الداتا اللي موجوده في الباكيت ممكن ننفذ نفس الامر السابق كالاتي

كود:PHP
```
/usr/local/snort/bin/snort -vd
```

ولاظهار الباكيت كامله .. الهيدر بالداتا فممكن ننفذ الاداه كالتالي:

كود:PHP
```
/usr/local/snort/bin/snort -vde
```

لو حبينا نعمل Logging للداتا في ملف تكست ومراجعتها لاحقا بدل من عرضها على الشاشه .. ممكن عن طريق الامر التالي:

كود:PHP
```
/usr/local/snort/bin/snort -vde -l /var/log/snort
```

لكن مشكلة ال Logging في ملف تكست بيسبب حمل على الشبكة وومكن يأدي الى بطء في الترافيك .. والحل انك بدل ما تعمل Logging في ملف تكست .. نعمل Logging لكن في ملف بينري bainaryكالتالي:

كود:PHP
```
/usr/local/snort/bin/snort -vde -l /tmp/ -b
```

ولقرائه الملف فيما بعد .. عن طريق الامر التالي:

كود:PHP
```
/usr/local/snort/bin/snort -r /tmp/snort.log.1097383338
```

طبعا الرقم ١٠٩٧٣٨٣٣٣٨ يختلف، مش واحد ينسخ الامر بالحرف ويقولي الملف مش موجود .. لانه دليل على رقم العملية فقط

وممكن تحدد من الملف البينري داتا معينه يظهرها .. يعني مثلا لو حبيت باكيت tcp فقط .. هيكون كالاتي:

كود:PHP
```
snort -dev -r /tmp/snort.log.1037840339 tcp
```

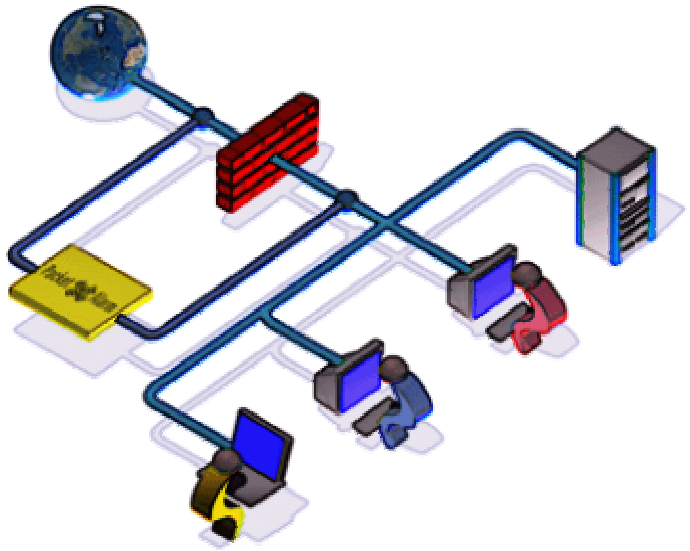
ايضا بأمكانك تشغيل Snort في packet sniffer mode و NIDS mode في نفس الوقت كالاتي:

كود:PHP

```
/usr/local/snort/bin/snort -dev -l /var/log/snort -c
/etc/snort/snort.conf
```

نقطة اخيرة احب اتكلم عنها قبل ماندخل في ال Rules وهي عن تهيئة Snort للعمل في شبكة على جهاز خاص.
افضل واامن طريقة لتشغيل Snort في شبكة انك تشغله في.Stealth Mode
حد عارف ايه هوStealth Mode ؟
بأختصار شديد Stealth Mode يجعل Snort sensor او الجهاز اللي عليه Snort غير مرئي للمهاجمين او لاي شخص في الشبكة اللي فيها .. Snort وهناك عدة طرق لوضع Snort في .. Stealth Mode
ابسطها:
انك لا تضع لكارت الشبكة .. IP address يعني تشغل الكرت عادي جدا بدون اعدادت الIP address وسيظل كارت الشبكة بعمل sniff والتقاط الباكيت .. لان عملية ال sniff ليس لها دخل بال IP address لكن هي تعتمد فقط ان كارت الشبكة متصل بشبكة فيها باكيتس رايحه وجاية وهو كل اللي عليه يلتقطهاز
المهم .. هناك حالتين ممكن تشغل بيها ال network interface بدون .. IP address وهما:
انك تشغل Snort sensor على كرت شبكة واحد بدون.IP address
والحالة التانية ان يكون عندك كرتين شبكة .. فهتشغل الكرت eth1 وتربطه مع الشبكة الداخلية وتديله IP addressمن ايبيهات الشبكة .. لكي تستطيع الدخول على الجهاز من الشبكة والتحكم به .. اما الكرت التاني eth0 فده وصله بال public network وخليه بدون IP address وده هو اللي هيتسخدم في جمع الباكيت وتحليلها

شوفو مثلا المثال في الصورة التالية
الصورة الوحيده اللي طلعهالي جوجلStealth Mode



نلاحظ ان Snort اللي باللون الاصفر له كرتين .. الكرت الاول متصل بالراوتر اللي موجود قبل الفايروول .. يعني بيستقبل كل الترافيك اللي جاية من الانترنت ويحللها .. والكرت التاني متصل بسويتش في الشبكة الداخلية لكي يستطيع الادمين ادرتها.. وكل سنة وانتم طيبين

نبدء بئى في ال Rules وما ادراك ما الRules
في البداية قبل الشرح احب اوضح انك لازم تكون فاهم كويس ال TCP\IP ومكونات الباكيت من header وداتا وبروتوكلات ال اخره ... لو فيه حد بيقرا الدرس ميعرفش الحاجات دي انصحه ميكملش ويلغي من دماغه اللي قرأه فوق .. لاني انا متأكد انه مش هيستفيد حاجه.

ولو فيه حد فعلا مش ميعرفش بس عاوز يتعلم .. فنصيحتي انك TCP\IP من RFCs

على الاقل يكون اي واحد قاريء RFCs المهمة التالية:

INTERNET PROTOCOL (IP)
ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)
ftp://ftp.rfc-editor.org/in-notes/rfc792.txt

User Datagram Protocol (UDP)
ftp://ftp.rfc-editor.org/in-notes/rfc768.txt

TRANSMISSION CONTROL PROTOCOL (TCP)
ftp://ftp.rfc-editor.org/in-notes/rfc793.txt

ولو فاضين .. واكيد طبعا فاضيين .. يعني انتو وراكو ايه
في اوقات الفراغ ابئو اتسلو في قرائة RFCs على المسار التالي:
http://www.rfc-editor.org/rfc/

ومتخافوش مش هتاخد وقت .. هيا كلها سنتين تلاته عشرة وتخلصو نصهم
ابئو قابلوني

لكن صراحه RFCs تعتبر افضل شيء يمكن تقرأه

نكمل..
دي رسمه بسيطة تشرح مكونات اي .. Rule قعدت ارسم فيها ربع ساعه على الشيل .. بس ياريت
متطلعش من تحت لفوق هنا:

كود:PHP
```
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
_    ___________________________________
|         Rule Header          | |       Rule Options           |
|                      | |                        |
alert  tcp   any  any   ->   any   any (msg: "Ping with TTL=100";
ttl: 100;)

|       |    |    |      |    |       |
|             /       |       /
Actions   |    ||            ||
      | src-ip&port       | dst-ip&port
      Protocol          Direction
```

ده مثال ل Rule بسيط

كود:PHP
```
alert tcp any any -> any any (msg: "Ping with TTL=100"; ttl: 100;)
```

يقوم بعمل تحذير لاي باكيت tcp تمر .. طبعا ده معمول كمثال ولا يصلح لشيء عدا ذلك

اول كلمة في الرول alert اللي هو ال .. Action وال Actions ممكن يكون alert يعني تحذير يحطه في ملف /var/log/snort/alerts او الاكشن ممكن يكون .. log يعني مش تحذير ولكن هيحطه في ملفات اللوج .. او ممكن يكون pass يعني كأنك بتقوله متوجعش دماغك بفحصها ولا عمل تحذير وعديها بسلام .. وممكن يكون activate وده يعني رد فعل .. يعني مثلا ممكن لو تطابق ال Rule الفلاني مع باكيت فالاداه تقوم بفعل منعكس كمثلا ادراج امر اي بي تيبلز في الفايروول ليقوم بوظيفة ما مثل حجب الباكيت واللي جايين بعدها او اي شيء اخر

تاني كلمة tcp وهي تحددلي نوع البروتوكول .. ودي ممكن تكون.... ip , tcp , udp , icmp

الخانة التالته any تعني Source IP Address وده ممكن يكون اي بي مفرد او عنوان شبكة .. والخانة الرابعه تمثل ال Source port وده ممكن يكون بورت واحد او عدة بورتات او مجال من البورتات

الخانه الخامسة <- تحدد اي الطرفين السورس واي الوجهة .. يعني لو بئى كده -> يبئى تعكس كل حاجه .. بسيطة

الخانة السادسة any تمثل ال Destination IP Address وممكن تكون عنوان واحد او عنوان شبكة ايضا
الخانسة السابعه any تمثلDestination port

بعد كده بئى لحد نهاية الرول ده يسمى الRule Options

كده خلصنا ال Rules

لان كل المطلوب منك تفهم شكل ال Rule بعد كده تستخدم خبرتك في ال TCP\IP في صياغة الاف ال Rulesبراحتك
لا اكثر ولا اقل

على فكرة نسيت اقول ان ال Rules تحطها في ملف /usr/local/snort/etc/snort.conf حطها في اخر الملف افضل

ممكن ناخد شوية امثلة للRules

كود:PHP
```
alert icmp ![192.168.2.0/24,192.168.8.0/24] any -> any any
  (msg: "Ping with TTL=100"; ttl: 100;)
```

ال Rule السابق سيطبق على كل كل باكيت icmp معدا الباكيتس اللي صادره من 192.168.2.0/24,192.168.8.0/24وخلي بالك من علامة ! في الرول اللي تعني النفي

مثال اخر:

كود:PHP
```
alert tcp 192.168.2.0/24 23 <> any any
  (content: "confidential"; msg: "Detected confidential";)
```

فكرو فيه كده...
هو Rule سيطبق على جميع الترافيك الخارج او الداخل من اي Telnet server في الشبكة .. ولا حظو علامة <> اللي قلبت الموازين

مثال اخر

كود:PHP
```
log udp any !53 -> any any log udp
```

وده هايعمل logs لكل ال UDP traffic معدا اللي يكون ال source port لها53

مثال اخير بئى وهنخليه في ال Rule Options اللي فيها الشغل التقيل
تعالو ناخد مثال حقيقي يفيدنا في الشغل

مثلا ال Nmap لما تيجي تعمل سكان بتبعت TCP packet الى البورت ٨٠ مثلا مع ACK flag في الباكيت و sequence number صفر او ٠ .. وطبعا اكيد انتو عارفين ان الباكيت غير مقبوله .. لا مفيش باكيت تبدأ الاتصل بACK
فاللي هيعمله سيرفر المستقبل .. او زي مالبعض بيسميه السيرفر الضحية ..انه هايرفض الاتصال عن طريق انه يرجعلك .. RST packet وهنا اول مال Nmap يستقبل RST packet يعرف ان الهوست شغال وموجود على الشبكة اونلاين.
نظام ان Nmap بياخد السيرفر على عقله
المهم الطريقة دي بيستخدمها ال Nmap مع الهوستات اللي بترفض ICMP ECHO REQUEST ping packets

انا عاوز اقول بعد القصة دي كلها .. اننا ازاي نعمل Rule يمسك الحركه الارعه دي بكل بساطه هيكون كالتالي:

كود:PHP
```
alert tcp any any -> 192.168.1.0/24 any (flags: A; ack: 0; msg: "TCP ping detected";)
```

ودي بعض ال TCP flag اللي ممكن تستخدمها في تكوين الاوامر

FIN or Finish Flag F
SYN or Sync Flag S
RST or Reset Flag R
PSH or Push Flag P
ACK or Acknowledge Flag A
URG or Urgent Flag U
Reserved Bit 1 1
Reserved Bit 2 2

الحقيقة اني كنت عاوز اشرح كيف الاستفاده من Snort في شن هجوم معاكس ضد الفلود او DOS,DDOSاو حماية شبكتك من المواقع الاباحية عن طريق البحث في الباكيت .. لكن المشكلة انهم هياخدو وقت طويل .. وانا جبت اخري

وبالتالي انشاء الله في درس قادم {لكن مش وعد} اشرح باقي ال Rules بالاضافه الى كيفية استخدام Snortمع OpenSSL , SNMP , jpgraph , MySql , Apache بالاضافه ال input و output plug-ins
ونشرح ايضا كيفية استخدام ACID في جمع الداتا من الداتا بيس واستخدامها لعرضها على الوب كما تعمل.webmine

للاستفسار والنقاش: www.s4a.cc/forum في قسم اللينوكس ..

انصح المهتمين بالرجوع الى المراجع والمصادره التالية:

http://www.snort.org1. Snort web site at
http://www.simpletimes.com2. SNMP
http://winpcap.polito.it/3. Winpcap Library
http://www.apache.org4. Apache
http://www.argusnetsec.com5. Argus Network Security Services Inc.
http://www-nrg.ee.lbl.gov/6. Libpcap
http://www.packetfactory.net7. Libnet
ftp://ftp.isi.edu/in-notes/rfc792.txt8. RFC 792 at
ftp://ftp.isi.edu/in-notes/rfc791.txt9. RFC 791 at at