الشرح العربي الرسمي للـ Snort

الكاتب : Super Linux

http://www.security4arab.net

ماهو الـ**Snort IDS ?**

محلل حقيقي للحزم الشبكيه او مايسمى باللـ **Packet** ويقيك من انواع عده من الاتتاك مثل البفر اوفر فلو وعمليات المسح الشبكي (سكان بورت) والـ **CGI Attacks** والـ **SMB probes** وايضاً **OS fingerprinting attempts** والكثير**..**

طبعاً شرحي مخصص لأنظمة الردهات فقط ،،

ابدا بالشرح الان

اولا نقوم بتغيير بورتكول الـ **SSH** من **1** الى **2**

اول قم بتحرير ملف الـ **/etc/ssh/sshd_config** باستخدام المحرر الى تفضله ومن ناحيتي افضل الـ **nano**

كود:**HTML**

```
pico /etc/ssh/sshd_config
```

قم بالبحث على**#Protocol 2,1**

وامسح الـ # الموجوده بجانبه ورقم **1** والفاصله **,**

لكي يظهر بهذا الشكل

Protocol 2

قم بحفظ عملك

كود:**HTML**

```
CTRL + X and press Y and Entre
```

بعد الانتهاء

قم بعمل رستارت للـ **SSH**

كود:**HTML**

```
root@server [~]# service sshd restart
```

```
Stopping sshd:[  OK  ]
Starting sshd:[  OK  ]
```

الان لنقم بانشاء مجلد في الرووت باسم**snort**

كود:**HTML**

```
root@server [~]# mkdir snort ; cd snort
root@server [~/snort]#
```

الان نقوم بانزال السنورت والعديد من المكتبات والملفات الي يحتاجها السنورت

اولا نقوم بانزل السنورت

كود:**HTML**

```
wget http://www.snort.org/dl/snort-2.1.3.tar.gz
```

كود:**HTML**

```
wget http://phplens.com/lens/dl/adodb390.tgz
```

كود:**HTML**

```
wget http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz
```

كود:**HTML**

```
wget http://www.gzip.org/zlib/zlib-1.2.1.tar.gz
```

كود:**HTML**

```
wget http://www.aditus.nu/jpgraph/downloads/jpgraph-1.13.tar.gz
```

كود:**HTML**

```
wget http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz
```

كود:**HTML**

```
wget http://unc.dl.sourceforge.net/sourceforge/pcre/pcre-4.1.tar.gz
```

الان قمنا بانزال السنورت وجميع مايحتاجه من مكتبات وملفات

اولاً نقوم بتنصيب الـ **Zlib** عن طريق الامر التالي

كود:**HTML**

```
tar -xvzf zlib-1.2.1.tar.gz
cd zlib-1.2.1
./configure
make
make install
cd ..
```

الان نقوم بتنصيب الـ**Libpcap**

كود:**HTML**

```
tar –xvzf libpcap-0.7.2.tar.gz
cd libpcap-0.7.2
./configure
make
make install
cd ..
```

الان نقوم بتنصيب الـ**pcre**

كود:**HTML**

```
tar -xvzf pcre-4.1.tar.gz
cd pcre-4.1
./configure
make
make install
cd ..
```

الان نقوم بتنصيب الـ**Snort**

كود:**HTML**

```
groupadd snort
useradd -g snort snort
mkdir /etc/snort
mkdir /var/log/snort
tar -xvzf snort-2.1.3.tar.gz
cd snort-2.1.3
./configure --with-mysql=/usr/local/mysql
make
make install
```

الان نقوم بنسخ ملفات الكونفج الى مجلداتها الرئيسيه

كود:**HTML**

```
cp * /etc/snort
cd ../etc
cp snort.conf /etc/snort
cp *.config /etc/snort
```

الان نقوم بالتعديل في اعدادات الـ **Snort**

كود:**HTML**

```
pico /etc/snort/snort.conf
```

اذا كنت تملك شبكه داخليه بين اجهزتك او سيرفراتك

قم بالبحث عن**var HOME_NET 10.2.2.0/24**

وقم بتغيير الـ **ips** حسب الايبيات الداخليه لسيرفراتك وليس الايبيات الخارجيه

من ناحيتي انا سويتها مثل كذا

var HOME_NET 192.168.1.1/2

بعدها قم بتغيير الـ**Rule Path**

من **var RULE_PATH ../rules** الى**/etc/snort/**

الان نقوم بالبحث عن**output database: log, mysql**

ثم تعديل الاعدادات فيه مثل السطر الى تحت

كود:**HTML**

```
output database: log, mysql, user=snort password=test dbname=snort
host=localhost
```

قم بتغيير الباسورد الى باسورد الرووت الخاص بالـ **Mysql**

الان في نفس السطر الى عدلنا فيه قم بحذف علامه الـ **#**

قم بحفظ عملك الان**CTRL + X and press Y and press Entre**

الان من سطر الاوامر قم بالدخول الى الـ **Mysql**

كود:**HTML**

```
root@server [~/snort/snort-2.1.3/etc]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 831 to server version: 4.0.20-standard

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

الان لنقم بانشاء قواعد البيانات

كود:**HTML**

```
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('test');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

الان قم بتنفيذ هذا الامر

كود:**HTML**

```
mysql -uroot -ppass snort < contrib/create_mysql
```

ملاحظه الـ **pass** بدله بباسورد الرووت الخاص بالـ**Mysql**

عد اضافه القاعده الان نقوم بالتاكد من ولوجها لقاعده البيانات

كود:**HTML**

```
root@server [~/snort/snort-2.1.3]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 840 to server version: 4.0.20-standard

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----------+
| Database  |
+-----------+
| eximstats |
| mail      |
| mysql     |
| snort     |
| test      |
+-----------+
5 rows in set (0.04 sec)

mysql> use snort;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.01 sec)

mysql> quit
Bye
root@server [~/snort/snort-2.1.3]#
```

الان نقوم بتركيب الـ **JPGraph** والـ **adodb** والـ**acid**

كود:**HTML**

```
tar -xvzf jpgraph-1.13.tar.gz
cp -rf jpgraph-1.13 /home/site/www/
tar -xvzf adodb390.tgz
cp -rf adodb /home/site/www/
tar -xvzf acid-0.9.6b23.tar.gz
cp -rf acid /home/site/www
```

الان نقوم بالتعديل في اعدادات الـكونفق الخاصه بالاسكربت الي قمنا بنقله لمجلد الموقع

كود:**HTML**

```
pico /home/site/www/acid/acid_conf.php
```

تعدل المهم الى فيه

عدل الـ

كود:**HTML**

```
$DBlib_path = "/home/site/www/adodb";
```

ملاحظه بدل الـ **site** لازم تحط مجلد الموقع الخاص فيك

كود:**PHP**

```
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "root";
$alert_password = "pass";

/* Archive DB connection parameters */
$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "root";
$archive_password = "pass";
```

غيرها حسب المعلومات الى انت اخترتها ولاتنسى باسورد الـ **root** او الـ **snort** لل**MySQL**

وقم بالبحث عن**$ChartLib_path**

وقم بتعديله الى الباث الخاص بموقعك مثال السطر الى تحت

كود:**HTML**

```
$ChartLib_path = "/home/site/www/jpgraph-1.13/src";
```

الان قم بحفظ عملك**CTRL + X And Press Y And Press Entre**

اذهب من المتصفح

http://ursite.com/acid/acid_main.php

واختار من تحت الـ **Setup Page** وبعدها **Create Acid**

والان لم يبقى الى ربط السنورت بالكورن لكي يعمل بعد اعاده تشغيل السيرفر

بكل بساطه قم بالرجوع للمجلد الي انشئناه الخاص بالـ **snort** في مجلد الرووت

cd /root/snort/snort-2.1.3

كود:**HTML**

```
cd /root/snort/snort-2.1.3
cp contrib/S99snort /etc/init.d/snort
```

بعدها قم بالتعديل ملف السنورت

كود:**HTML**

```
pico /etc/init.d/snort
```

بعدها قم بتعديل الـ **CONFIG=** الى

كود:**HTML**

```
CONFIG=/etc/snort/snort.conf
```

وتعديل الـ **SNORT_GID=** الى

كود:**HTML**

```
SNORT_GID=snort
```

قم بحفظ عملك**CTRL + X And Press Y And Press Entre**

بعدها قم بتفيذ هذه الاوامر

كود:**HTML**

```
cd /etc/init.d
chmod 755 snort
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
```

واخيراً

snort –c /etc/snort/snort.conf

هذا الامر لتجربه عمل السنورت

تحياتي كاتب الموضوع**Super Linux**

ملاحظه : الموضوع مطبق كاملاً وقد اعتمدت على بعض المصادر في تكويني لهذا الموضوع الطويل المتكامل واعتبره اول موضوع عربي يشرح الـ **snort** من الف الى ياء

تحياتي**Super Linux**