



Manual de Instalação do Snort@Ubuntu

Snort, Apache, PHP, MySQL, BASE @ Ubuntu

+

Guardian

Setembro, 2006
Versão 1.0

Elaborado por:

- Miguel Sampaio (miguelsaraiva@zmail.pt)
- Marco Silva (mareco@portugalmail.pt)

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
www.estg.ipleiria.pt

I. Agradecimentos

Este trabalho foi realizado no âmbito da disciplina de Projecto I, da Licenciatura em Engenharia Informática e Comunicações (EIC), da Escola Superior de Tecnologia e Gestão (ESTG), do Instituto Politécnico de Leiria (IPL).
A orientação do projecto esteve a cargo dos professores Mário Antunes e Miguel Frade que contribuíram na fase de edição deste documento.

II. Introdução

Este manual pretende apresentar, de uma forma simples, o processo de instalação de um sensor do *Network Intrusion Detection System (NIDS)* Snort e de todos os componentes de *software* necessários. Este trabalho insere-se no âmbito do desenvolvimento de um projecto de avaliação das funcionalidades do Snort, recorrendo à realização de testes numa rede piloto. A instalação em que se baseou este manual decorreu numa máquina com o sistema operativo Ubuntu 5.10 já instalado e com o servidor X também instalado e configurado.

III. Requisitos

Antes de iniciar a instalação e configuração do Snort e de alguns dos seus utilitários, é necessário instalar algum software fundamental.

1 Instalar PHP, MySQL e Apache

1.1 Por *download* e instalação manual:

- PHP (www.php.net)
- MySQL (www.mysql.com)
- Apache (www.apache.org)

1.2 Via apt-get:

```
# sudo apt-get install apache2
# sudo apt-get install mysql-server
# sudo apt-get install php5
# sudo apt-get install php5-mysql
```

2 Configurar o “iptables” para que, especialmente na fase de testes, não bloqueie o tráfego IP.

```
# sudo iptables -I INPUT -i eth0 -p ip -j ACCEPT
```

3 Testar o Apache através do seguinte código php:

```
# sudo nano /var/www/index.php

<?php
phpinfo();
?>
```

Após a instalação do Apache, deverá ser possível aceder através de um *browser* aos seguintes recursos: http://127.0.0.1/ ou http://localhost/.

4 Instalar o ADODB e o BASE (Basic Analysis and Security Engine) disponíveis respectivamente em:

- http://prdownloads.sourceforge.net/adodb/
- http://prdownloads.sourceforge.net/secureideas/

IV. Instalar o Snort

1. Executar o *download* do Snort e do PCRE:
   - http://www.snort.org
   - http://prdownloads.sourceforge.net/pcre/

2. Através do utilitário "Adept" verificar se estão instalados os componentes libpcap0.8, libpcap0.8-dev, libpcre3 e o libpcre3-dev, necessários para a instalação do Snort. Se necessário, proceder à sua instalação via Adept.

3. Instalar PCRE

   ```
   # sudo tar -xvzf pcre-6.3.tar.gz
   # cd pcre-6.3
   # sudo ./configure
   # sudo make
   # sudo make install
   ```

4. Instalar Snort

   ```
   # sudo tar -xvzf snort-2.4.4.tar.gz
   # cd snort-2.4.4
   # sudo ./configure --with-mysql=<localização do mysql>
   # sudo make
   # sudo make install
   ```

   Se ocorrer a seguinte mensagem de erro: *"snort: error while loading shared libraries: libpcre.so.0: cannot open shared object file: No such file or directory"*, deverá criar-se um link simbólico, através do seguinte comando:

   ```
   # sudo ln -s /usr/local/lib/libpcre.so.0 <localização do ficheiro>
   ```

   Por exemplo:

   ```
   # sudo ln -s /usr/local/lib/libpcre.so.0 /usr/lib/libpcre.so.0
   ```

5. Efectuar o *download* das regras e proceder á sua extracção para a directoria "/etc/snort/rules"

6. Configurar os seguintes parâmetros no ficheiro "/etc/snort/snort.conf":

   ```
   var HOME_NET any (Para capturar todos as redes)
   var EXTERNAL_NET !$HOME_NET (Tudo o que não for HOME_NET é externo)
   var RULE_PATH /etc/snort/rules (caminho correcto para as regras)
   --preprocessor
   output database: log, mysql, user=snort password=<pwd_escolhida>
   ```

```
dbname=snort host=localhost
```

7. Configurar a base de dados do Snort no MySQL:

```
# mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('password');
>Query OK, 0 rows affected (0.25 sec)
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('password_do_snort.conf');
>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
```

8. Executar os seguintes comandos para criar as tabelas

```
# mysql -u root -p < ~/snortinstall/snort-2.4.3/schemas/create_mysql snort
Enter password: mysql root password
```

9. Verificar se a BD do Snort foi criada correctamente

```
# mysql -p
>Enter password:
mysql> SHOW DATABASES;

+------------+
| Database
+------------+
| mysql
| Snort
| test
+------------+
3 rows in set (0.00 sec)

mysql> use snort
>Database changed

mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
Version 13 Page 13 of 20 Updated 10/24/2005 7:39 PM
| event
| icmphdr
```

```
| iphdr
| opt
| reference
| reference_system
| schema
| sensor
| sig_class
| sig_reference
| signature
| tcphdr
| udphdr
+------------------+
16 rows in set (0.00 sec)
exit;
```

V. Instalar o ADODB:

```
# cp adodb462.tgz /var/www/
# cd /var/www/
# tar -xvzf adodb462.tgz
# rm –rf adodb462.tgz
```

VI. Instalar e configurar o BASE:

1. Instalar:

```
# cp base-1.2.tar.gz /var/www/html
# cd /var/www/html
# tar –xvzf base-1.2.tar.gz
# rm –f base-1.2.tar.gz
# mv base-1.2 base (renomear “base-1.2” para simplesmente “base”)
# cd /var/www/html/base
# cp base_conf.php.dist base_conf.php
```

2. Editar o ficheiro “/var/www/html/base/base_conf.php” e introduzir os seguintes parâmetros:

```
$BASE_urlpath = "/base";
$DBlib_path = "/var/www/adodb/";
$DBtype = "mysql";
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "password_do_snort_conf";
/* Archive DB connection parameters */
$archive_exists = 0; # Set this to 1 if you have an archive DB
```

VII. Iniciar o Snort

1. Activar o Snort para iniciar a recolha de tráfego, através da execução do seguinte comando:

```
# snort -c <ficheiro de configuração>
```

Por exemplo, para o ficheiro de configuração do Snort "`/etc/snort/snort.conf`", o arranque do Snort é efectuado pelo seguinte comando:

```
# snort -c /etc/snort/snort.conf
```

2. Consultar o BASE, executando num *browser*:

   `https://<endereço.ip>/base/html`

   Na página inicial de setup do BASE clicar no link *"setup page"* e de seguida no botão "*setup AG"*. Nesta altura é possível aceder e consultar os *logs* do Snort acedendo simplesmente ao endereço `https://<endereço.ip>/base/html`.

VIII. Instalar o Guardian

O Guardian é um programa que funciona em conjunto com o Snort. A sua função consiste na actualização automática das regras do "iptables", com base nos alertas gerados pelo Snort. A actuação conjunta do Snort e do Guardian torna possível dotar o Snort de mecanismos de reacção em caso de intrusão e prevenção de ataques futuros. De seguida são apresentados os passos para instalação deste programa:

1. Efectuar o *download* do Guardian em http://www.chaotic.org/guardian/.

2. Executar os seguintes comandos:

```
# mv guardian-x-x.tar.gz /usr/src
# tar -xvzf guardian-x-x.tar.gz
# cd guardian-x-x
# cd scripts
# ls
```

A directoria "scripts" deverá ter os seguintes *scripts*:

```
freebsd_block.sh        freebsd_unblock.sh      ipchain_block.sh
ipchain_unblock.sh      iptables_block.sh       iptables_unblock.sh
```

O programa Guardian utiliza sempre os *scripts* denominados *"guardian_block.sh"* e *"guardian_unblock.sh"*. Assim, deverão ser copiados para ficheiros com esses nomes os correspondentes ao filtro de pacotes que pretendemos utilizar. No caso concreto do "iptables" que é o mais frequentemente utilizado, deverão realizar-se os seguintes comandos:

```
# cp iptables_block.sh /usr/bin/guardian_block.sh
# cp iptables_unblock.sh /usr/bin/guardian_unblock.sh
# chmod 755 /usr/bin/guardian_block.sh /usr/bin/guardian_unblock.sh
```

3. Copiar o *script* e ficheiro de configuração do Guardian para os locais correspondentes, através dos seguintes comandos:

```
# cd ..
# cp guardian.pl /usr/bin
```

```
# chmod 755 /usr/bin/guardian.pl
# cp guardian.conf /etc/
```

4. Configurar os seguintes parâmetros no ficheiro "/etc/guardian.conf":
   - `Interface eth0 - interface eth0, a que vai ter os terminais bloqueados`
   - `AlertFile /var/adm/secure - mudar para /var/log/snort/alert`
   - `TimeLimit 86400 - mudar para um valor em segundos que pretendemos que o endereço IP fique bloqueado pela` *`firewall`*`. O valor "99999999" remove esta opção.`

5. Criar o arquivo de log do Guardian, através do comando:

```
# touch /var/log/guardian.log
```

6. Criar o ficheiro "guardian.ignore" com os endereços IP que se pretende ignorar:

```
# touch /etc/guardian.ignore
```

7. Iniciar o Guardian

```
# guardian.pl -c /etc/guardian.conf
OS shows Linux
Warning! HostIpAddr is undefined! Attempting to guess..
Got it.. your HostIpAddr is 192.168.1.1
My ip address and interface are: 192.168.1.1 eth0
Loaded 3 addresses from /etc/guardian.ignore
Becoming a daemon..
```

Versões:

V 1.0 Documento inicial