5.1 Instalace aplikace Snort a jejích součástí

Instalace open source IDS Snort nemůže být provedena prostým způsobem pomocí programů *aptitude* či *apt*, neboť ji chceme využívat jako IPS a je tedy nutné provést instalaci ze zdrojových kódů. Tato nutnost vzniká právě díky použití s aplikací *SnortSam*, která vyžaduje opatchování zdrojových kódů Snortu. Patch je dostupný na stránkách[2], bohužel však pouze pro verzi Snort 2.9.0.3 (v době testování již byla dostupná vyšší verze Snort 2.9.0.4, patch pro tuto verzi však nikoliv). Zdrojové kódy pro Snort tedy stáhneme prostřednictvím příkazu *wget* následujícím způsobem.

```
wget http://www.snort.org/dl/snort-current/snort-2.9.0.3.tar.gz
    -O snort-2.9.0.3.tar.gz
```

Tímto máme stáhnuté zdrojové kódy pro Snort, verze od 2.9.0 výše ale využívají nové daq, stáhneme tedy i tyto zdrojové kódy.

```
wget http://www.snort.org/downloads/860 -O daq-0.5.tar.gz
wget http://www.snortsam.net/files/snort-plugin/
    snortsam-2.9.0.3.diff.gz -O snortsam-2.9.0.3.diff.gz
wget http://www.snortsam.net/files/snortsam/
    snortsam-src-2.70.tar.gz -O snortsam-src-2.70.tar.gz
```

Poslední dva výše zmíněné přikazy stáhnou zdrojové kódy aplikace *SnortSam* i patch potřebný pro *Snort*. Další aplikací, jejíž zdrojové kódy potřebujeme, je *libdnet*. Je sice dostupný i ve formě balíčků, ale vhodnější je provést instalaci ručně.

```
wget http://libdnet.googlecode.com/files/libdnet-1.12.tgz
    -O libdnet-1.12.tgz
```

Nyní již máme k dispozici všechny zdrojové kódy pro kompilaci Snortu, musíme ale ještě doinstalovat aplikace, které jsou pro běh Snortu nezbytné, případně jsou nutné pro vlastní kompilaci. Tyto aplikace lze ale instalovat prostřednictvím systémového správce balíků.

- libpcap0.8-dev
- libpcap-dev
- libmysqlclient15-dev (libmysqlclient-dev)
- libmysqld-dev
- bison
- flex
- libapache2-mod-php5

[2] http://www.snortsam.net/download.html

- php5-gd
- php5-mysql
- libtool
- libpcre3-dev
- pcre-dev
- php-pear
- gcc
- automake
- autoconf
- apache2
- mysql-client-5.1
- mysql-server-5.1

Některé z těchto programů již mohou být nainstalovány (zvláště pak poslední trojice, díky možnosti LAMP při instalaci operačního systému), žádný z nich by však neměl chybět.

5.1.1 Kompilace a instalace daq

Probíhá obvyklým způsobem - rozbalením archívu a tzv. „svatou trojicí".

```
tar zxvf daq-0.5.tar.gz
cd daq-0.5
./configure
make
make install
```

5.1.2 Kompilace a instalace libdnetu

Stejný průběh jako u *daq*, posledním krokem je vytvoření symbolického linku.

```
tar zxvf libdnet-1.12.tgz
cd libdnet-1.12/
./configure
make
make install
ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1
```

5.1.3 Příprava zdrojových kódů Snortu, instalace SnortSam

Přejdeme do složky, kde máme stažený patch snortsam-2.9.0.3.diff.gz. Začneme rozbalením archívu.

```
gunzip snortsam-2.9.0.3.diff.gz
```

Nyní nastává čas na konfiguraci kódů Snortu a aplikaci rozbaleného patche. Pokud se patch pro snort nenachází o úroveň adresáře výše než snort, zadejte v příkazu *patch* cestu k tomuto souboru.

```
patch -p1 < ../snortsam-2.9.0.3.diff
bash ./autojunk.sh
./configure --enable-ipv6 --enable-gre --enable-mpls
    --enable-targetbased  --enable-decoder-preprocessor-rules
    --enable-ppm --enable-perfprofiling --enable-zlib
    --enable-active-response --enable-normalizer --enable-reload
    --enable-react --enable-flexresp3 --with-mysql
make
make install
groupadd snort
useradd -g snort snort
mkdir /var/log/snort
chown snort:snort /var/log/snort
mkdir /etc/snort
mkdir /etc/snort/rules
cd rules/
cp * /etc/snort/rules
cd ../etc/
cp * /etc/snort/
```

Aplikaci SnortSam pak doinstalujeme následovně. Ve složce s rozbalenými kódy spustíme tyto příkazy.

```
chmod -x makesnortsam.sh
./makesnortsam.sh
cp snortsam /usr/bin/
```

V době testování byla používána verze 2.70

5.1.4 Konfigurace Snortu

Konfigurační soubor nacházející se v */etc/snort/snort.conf* musíme mírně upravit. Nastavíme proměnné *HOME_NET* a *EXTERNAL_NET*, zavedeme nové proměnné pro SIP proxy server.