

NetFlow - PortTracker Exercises

Optional Tasks

Installing the PortTracker plugin (Optional or as reference)

We need to get nfdump 1.6.5 or newer. The version of nfdump included in Ubuntu 10.04 is 1.6.3p1, so that won't work.

```
~~~~~
# cd /usr/local/src
# wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.6.tar.gz
# tar xvzf nfdump-1.6.6.tar.gz
# cd nfdump-1.6.6
# ./configure --prefix /usr --enable-nfprofile --enable-nftrack
# make
# make install
~~~~~
```

* Make a directory for the nftrack data

```
~~~~~
$ sudo mkdir -p /var/log/netflow/porttracker
$ chown www-data /var/log/netflow/porttracker
~~~~~
```

* Set the nftrack data directory in the PortTracker.pm module:

```
~~~~~
$ editor extra/PortTracker.pm
```

Find the line:

```
my $PORTSDBDIR = "/data/ports-db";
```

and change it to:

```
my $PORTSDBDIR = "/var/log/netflow/porttracker";
~~~~~
```

...

* Install the plugins into the NFSen distribution

```
~~~~~
$ cp extra/PortTracker.pm /var/nfsen/plugins/
$ cp /usr/local/src/nfsen-1.3.6p1/contrib/PortTracker/PortTracker.php \
  /var/www/nfsen/plugins/
~~~~~
```

* Add the plugin definition to the nfsen.conf configuration

```
~~~~~
$ cd /usr/local/src/nfsen-1.3.6p1
$ editor etc/nfsen.conf
~~~~~
```

Find the plugins section and make it look like this:

```
~~~~~
@plugins = (
    [ 'live',    'PortTracker'],
);
~~~~~
```

...

* Re-run the installation (answer questions)

```
~~~~~  
$ perl install.pl etc/nfsen.conf  
~~~~~
```

* Initialize porttracker database files

```
~~~~~  
$ sudo -u www-data nftrack -I -d /var/log/netflow/porttracker  
~~~~~
```

(This can take a LONG time! - 8 GB worth of files will be created)

* Set the permissions so the netflow user running nfsen, and the www-data user running the Web interface, can access the porttracker data:

```
~~~~~  
$ chown -R netflow:www-data /var/log/netflow/porttracker  
$ chmod -R 775 /var/log/netflow/porttracker  
~~~~~
```

* Reload:

```
~~~~~  
$ /var/nfsen/bin/nfsen reload  
~~~~~
```

* Check for success:

```
~~~~~  
$ grep -i 'porttracker.*success' /var/log/syslog  
Nov 27 02:46:13 noc nfsen[17312]: Loading plugin 'PortTracker': Success  
Nov 27 02:46:13 noc nfsen[17312]: Initializing plugin 'PortTracker': Success  
~~~~~
```

* Wait some minutes, and go to the nfsen GUI

```
~~~~~  
http://pcX.ws.nsrc.org/nfsen/nfsen.php  
~~~~~
```

... and select the Plugins tab.

If you get an error "Cannot Read Stats file", check the /var/log/netflow/porttracker \ directory for 2 additional files: portstat24.txt and portstat.txt like this:

```
~~~~~  
$ ls -l /var/log/netflow/porttracker/portstat*  
-rw-r--r-- 1 netflow www-data      677 2011-11-17 14:30 /var/log/netflow/\  
porttracker/portstat24.txt  
-rwxrwxr-x 1 netflow www-data      638 2011-11-17 14:30 /var/log/netflow/\  
porttracker/portstat.txt  
~~~~~
```

Make sure that nfsen can write in that directory.

If you wanted to add more sources...

(Note, you should already have two sources and not need to do this step!)

Go back to where you extracted your nfsen distribution.

```
~~~~~  
$ cd /usr/local/src/nfsen-1.3.6pl  
$ editor etc/nfsen.conf  
~~~~~
```

Update your sources for new items that you might have.
(Sample only!)

```
~~~~~  
%sources = (  
'rtr' => { 'port' => '9000', 'col' => 'e4e4e4' },  
'rtr2' => { 'port' => '9001', 'col' => '#0000ff' },  
'rtr3' => { 'port' => '9002', 'col' => '#00cc00' },  
'rtr4' => { 'port' => '9003', 'col' => '#000000' },  
'rtr5' => { 'port' => '9004', 'col' => '#ff0000' },  
'rtr6' => { 'port' => '9005', 'col' => '#ffff00' },  
);  
~~~~~
```

Save and exit from the nfsen.conf file.

Remember, you've updated nfsen.conf so you must re-run the install
script:

```
~~~~~  
$ perl install.pl etc/nfsen.conf  
~~~~~
```

Now start and stop nfsen:

```
~~~~~  
$ sudo service nfsen stop  
$ sudo service nfsen start  
~~~~~
```

That's it!