Monitoring Netflow with NFsen

Contents

1 Introduction

1.1 Goals

- Learn how to install the nfdump and NfSen tools

1.2 Notes

- Commands preceded with "$" imply that you should execute the command as a general user - not as root.
- Commands preceded with "#" imply that you should be working as root.
- Commands with more specific command lines (e.g. "rtrX>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

2 Configure Your Collector

2.1 Install NFDump and associated software

NFdump is part of the Netflow flow collector tools, which includes:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

We install this in the usual way:

```
$ sudo apt-get install nfdump
```

2.1.1 Testing nfcapd and nfdump

```
$ mkdir /tmp/nfcap-test
$ nfcapd -E  -p 9001 -l /tmp/nfcap-test
```

... after a while, a series of flows should be dumped on your screen.

Stop the tool with CTRL+C, then look at the contents of /tmp/nfcap-test

```
$ ls -l /tmp/nfcap-test
```

You should see one or more files called `nfcapd.<YEAR><MON><DAY><HR><MIN>`

Process the file(s) with nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyyzz -s srcip/bytes
```

You should get some useful information :)

2.2 Install apache2

Make sure apache is running on your workstation before you fo any further. If you need to install it:

```
$sudo apt-get install apache2
```

2.3 Installing and setting up NfSen

Download and compile. We need to install two patches as part of the process.vm

```
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
$ tar xvzf nfsen-1.3.6p1.tar.gz
$ cd nfsen-1.3.6p1
$ wget http://noc.ws.nsrc.org/downloads/nfsen-lookup.patch
$ patch -p0 < nfsen-lookup.patch
$ wget http://noc.ws.nsrc.org/downloads/nfsen-socket6.patch
$ patch -p0 < nfsen-socket6.patch
$ cd etc
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
```

Set the $BASEDIR variable

```
$BASEDIR = "/var/nfsen";
```

Set the users appropriately so that Apache can access files:

```
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
```

Set the buffer size to something small, so that we see data quickly. You would not do this on a production system.

Set the nfdump tools path

```
$PREFIX  = '/usr/bin';
```

Receive buffer size for nfcapd - see man page nfcapd(1)

```
$BUFFLEN = 2000;
```

Find the %sources definition, and change it to:

```
%sources=(
'rX1' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
 );
```

(substitute your group's router for rX1, and either remove or comment out the existing sample sources). Now save and exit from the file.

Finally, as this is Ubuntu 14.04, change the HTMLDIR from `/var/www/nfsen/` to `/var/www/html/nfsen/`

```
$HTMLDIR    = "/var/www/html/nfsen/";
```

2.4 Create the netflow user on the system

```
$ sudo useradd -d /var/nfsen -G www-data -m -s /bin/false netflow
```

2.5 Install NfSen and start it

Change directory back to just inside the source directory:

```
$ cd
$ cd nfsen-1.3.6p1
```

Now, finally, we install:

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

Press ENTER when prompted for the path to Perl.

2.6 Install init script

In order to have nfsen start and stop automatically when the system starts, add a link to the init.d diretory pointing to the nfsen startup script:

```
$ sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
$ sudo update-rc.d nfsen defaults 20
```

Start NfSen

```
$ sudo service nfsen start
```

Check that nfcapd processes have been started:

```
$ ps auxwww | grep nfcapd
```

2.7 View flows via the web:

You can find the nfsen page here:

`http://vmX.ws.nsrc.org/nfsen/nfsen.php`

If you are working in pairs, then both of you should point your web browser to the PC which is receiving flows.

You may see a message such as:

`Frontend - Backend version mismatch!`

This will go away if you reload the page, it's not a problem.

Done! Move on to the third lab, exercise3-nfsen-top-talkers

- NOTES:

2.8 Adding sources

If you had multiple routers in your network all sending flows to the same collector, you can either configure them to send to different ports on the collector, or you can tell nfsen the source IP address of each router. This allows nfsen to show distinct data from each source.

DON'T DO THIS NOW as you only have a single router, but if you needed to, you would do it as follows:

- edit /var/nfsen/etc/nfsen.conf, and add the source(s), for example:

```
%sources = (
    'rtrX'  => { 'port' => '9001', 'col' => '#0000ff', 'type' => 'netflow' },
    'rtrY'  => { 'port' => '9002', 'col' => '#00ff00', 'type' => 'netflow' },
    'gw'    => { 'port' => '9996', 'col' => '#ff0000', 'type' => 'netflow' },
);
```

- Reconfigure NfSen.

You will need to run this every time you modify `/var/nfsen/etc/nfsen.conf`:

```
$ sudo /etc/init.d/nfsen reconfig
```

You should see:

```
New sources to configure : gw rtrY
Continue? [y/n] y

Add source 'gw'
Add source 'rtrY'

Start/restart collector on port '9002' for (rtr2)[pid]
Start/restart collector on port '9996' for (gw)[pid]

Restart nfsend:[pid]
```