Install nfdump/nfSen

Introduction

Goals

- Learn how to install the nfdump and NfSen tools

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.

Configure Your Collector

Install NFDump and associated software

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

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

This is already installed on your srv1 instance, so you can proceed straight to the next step.

Testing nfcapd and nfdump

Log into your campus “srv1” instance, and run the following (you don’t have to be “root” to do this):

```
$ mkdir /tmp/nfcap-test
$ nfcapd -E -p 9996 -l /tmp/nfcap-test
```

There is an initial response:

```
Bound to IPv4 host/IP: any, Port: 9996
Startup.
Init IPFIX: Max number of IPFIX tags: 79
```

… after a while, a series of flows should be dumped on your screen, for example

```
Process_v9: New exporter: SysID: 1, Domain: 0, IP: 100.68.6.1

Process_v9: [0] Add template 256

Flow Record:
  Flags        =              0x06 NETFLOW v9, Unsampled
  label        =            <none>
  export sysid =                 1
  size         =                92
  first        =        1664982511 [2022-10-05 15:08:31]
  last         =        1664982546 [2022-10-05 15:09:06]
  msec_first   =               965
  msec_last    =                 2
  src addr     =        100.64.0.1
  dst addr     =      100.68.6.130
  src port     =             33498
  dst port     =                22
...
```

These are actually decoded netflow records - for example you can see the source and destination IP addresses and ports for a particular flow.

Once you've received a few flow records, stop the tool with CTRL+C, then look at the files inside the directory `/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.20YYwwxxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.20YYwwxxyyzz -s srcip/bytes
```

You should get some useful information :) The first command shows individual flows. The second aggregates them, so you get row for each source IP address, showing the total number of bytes across all flows with that source IP.

Install NfSen

NfSen has been installed and configured for you.

Configure timezone

WARNING: This exercise assumes that you have left the timezone on your srv1 server set to UTC. If this is true, then skip to the next section.

If not, then you will need to make an additional change to make NfSen work properly. First check what version of PHP you are running: e.g.

```
$ ls /etc/php
8.1
```

Then create the following config file (replacing “8.1” if necessary):

```
$ sudo editor /etc/php/8.1/apache2/conf.d/90-timezone.ini
```

The contents of this file should be a single line which sets `date.timezone` to the correct timezone name (https://www.php.net/manual/en/timezones.php) , which is usually the same as you had chosen with dpkg-reconfigure tzdata, for example:

```
date.timezone = Africa/Kigali
```

Save this file, then restart apache:

```
systemctl restart apache2
```

Configure NfSen

View the file `/var/nfsen/etc/nfsen.conf` in an editor or using `less` , and check there is a section that looks like this:

```
%sources = (
# Examples:
#    'upstream1'    => { 'port' => '9995', 'col' => '#0000ff',
'type' => 'netflow' },
#    'peer1'        => { 'port' => '9996', 'IP' =>
'172.16.17.18' },
#    'peer2'        => { 'port' => '9996', 'IP' =>
'172.16.17.19' },
  'bdr1' => {'port'=>'9996', 'col'=>'#0000ff',
'type'=>'netflow'},
);
```

This means that it’s expecting to receive netflow packets on (UDP) port 9996, and that these will be labeled as “bdr1” and graphs will be blue. This is where you would add extra sources of

NetFlow data.

Start NfSen

Run the following. It will start both the nfsen server process and nfcapd process(es) for all the configured sources of NetFlow data.

```
$ sudo systemctl enable nfsen
$ sudo systemctl start nfsen
```

Check that an nfcapd process has been started:

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

You should see something similar to:

```
netflow     9633  0.0  0.1  24836  2592 ?        S    15:26
0:00 /usr/local/bin/nfcapd -w -D -p 9996 \
-u netflow -g www-data -B 20000 -S 1 -P
/var/nfsen/var/run/p9996.pid -z -I bdr1 -l /var/nfsen/profiles-
data/live/bdr1
```

You can see which port it's listening on (`-p 9996`) and which directory it's writing files to (`-l`)

View flows via the web:

You can find the nfsen page here:

```
http://oob.srv1.campusY.ws.nsrc.org/nfsen/nfsen.php
```

Everyone in your group should point their web browser to the same URL.

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

Note that the graphs will take at least 5 minutes to start showing anything, since this is how often nfcapd rotates its log files and updates graphs. (Each point on the graph is a *summary* of all the flows in that 5 minute period)

NOTES

These are for future reference.

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, 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 = (
    'bdr1_campusY'  => { 'port' => '9996', 'col' =>
'#0000ff', 'type' => 'netflow' },
    'core1_campusY'  => { 'port' => '9997', 'col' =>
'#00ff00', 'type' => 'netflow' },
    'transit1_nren'    => { 'port' => '9998', 'col' =>
'#ff0000', 'type' => 'netflow' },
);
```

  Colors are in the HTML/CSS format (hex RRGGBB).

- 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 : core1.campusY, transit1.nren
Continue? [y/n] y

Add source 'core1.campusY'
Add source 'transit1.nren'

Start/restart collector on port '9002' for (core1.campusY)
[pid]
Start/restart collector on port '9996' for (transit1.nren)
[pid]
```

```
Restart nfsend:[pid]
```

Installation Reference

The remainder of this document is a reference in case you want to install these tools at home.

nfdump

There is a package in Ubuntu, but it's not the most recent, so it's preferable to build it from source.

First, check you have the build tools and dependencies (these include the dependencies required by nfSen as well):

```
$ sudo apt-get update
$ sudo apt-get install build-essential autoconf libtool pkg-
config
$ sudo apt-get install rrdtool librrds-perl librrdp-perl librrd-
dev libbz2-dev \
       libmailtools-perl libsocket6-perl apache2 libapache2-mod-
php bison flex
```

Now proceed to download and build. Note that only the last step (make install) has to be done as root.

```
$ cd
$ wget https://github.com/phaag/nfdump/archive/v1.7.2.tar.gz
$ tar -xvzf nfdump-1.7.2.tar.gz
$ cd nfdump-1.7.2
$ ./autogen.sh
$ ./configure --help      # optional, shows the build settings
available
$ ./configure --enable-nfprofile --enable-nftrack
$ make
$ sudo make install
$ sudo ldconfig
```

This will install the tools under `/usr/local/bin` and `/usr/local/lib` .

NfSen

Downloading and configuring NfSen

Download and unpack. Although NfSen is not being actively developed, there is a version on github which has been updated to work with nfdump 1.7 and PHP 8.1 (which is in Ubuntu 22.04)

```
$ cd
$ wget https://github.com/phaag/nfsen/archive/v1.3.9.tar.gz
$ tar -xvzf nfsen-1.3.9.tar.gz
$ cd nfsen-1.3.9/etc
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
```

Set the $BASEDIR variable

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

Change the HTMLDIR from `/var/www/nfsen/` to `/var/www/html/nfsen/`

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

Set the users appropriately so that Apache can access files:

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

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

```
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;
```

Find the %sources definition, and change it to:

```
%sources=(
'bdr1_campusY' =>
{'port'=>'9996','col'=>'#0000ff','type'=>'netflow'},
);
```

(substitute your group's router for bdr1_campusY, and either remove or comment out the existing sample sources).

Now save and exit from the file.

Create the netflow user on the system

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

Install NfSen and start it

Change directory back to just inside the source directory:

```
$ cd
$ cd nfsen-1.3.9
```

Now, finally, we install:

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

Press ENTER when prompted for the path to Perl.

If you get this error:

> *Can not get semaphore: at libexec/Nfsync.pm line 48.*

then just repeat the command.

Install init script

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

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