Lab 11.1 Introduction to Snort
IN715 Networks Three

October 14, 2014

Introduction

Snort is a powerful network traffic analysis tool. It has the capacity to

- sniff network packets in real time;
- log packet data to a file;
- analyse captured packets for intrusion dectection.

Ultimately it is the last item that is most interesting to us.

Carry out this lab on your `router2` system.

1 Install and try Snort

Installation on our OpenBSD servers is extremely easy. Just enter the command

```
pkg_add snort
```

and it will be installed.

Try out Snort by having it sniff packets and output its data to the console with the following command.

```
snort -v --daq-dir/usr/local/lib/daq
```

Information about packets will be displayed in the console. Carry out some network activity to generate some interesting packets to log. Enter `Ctrl-c` to stop Snort when you are done. If you want to see the packet payload data as well, invoke Snort with the -d option:

```
snort -dv --daq-dir/usr/local/lib/daq
```

2 Logging Snort data to a file

In a typical network setting Snort will capture too much data to be usefull examined in standard output. It is more productive to have Snort write its data to a logfilethat we can examine later. We can do this by using Snort's `-l` option, like this:

```
mkdir log
snort -dv -l ./log --daq-dir/usr/local/lib/daq
```

Snort will then write its data into a file in the `log` directory. This logfile is in a binary format that can be read with tools like `tcpdump` or with snort itself. After having Snort log for a few minutes, stop Snort by entering `Ctrl-c`. Then you can inspect the logged data by converting it to a text file with a command like this:

```
snort -dv --daq-dir/usr/local/lib/daq -r ./log/<log file name>   > snort_log
```

Now the file `snort_log` contains the data in text format.

3 Running the Snort service

To use Snort as a proper *Network Intrusion Detection System* (NIDS), we need to install some processing rules that identify packets of interest. Rather than log every packet seen, we want to indentify those that match a suspected attack signature. We can write our own rules, but it's best to start with a standard set.

First, make a directory to store our rules:

```
mkdir /usr/local/snort
cd /usr/local/snort
```

Now download some rules an unpack them.

```
pkg_add curl
curl http://kate.ict.op.ac.nz/~tclark/snortrules.tgz > snortrules.tgz
tar -xzf snortrules.tgz
```

Now you need to modify the configuration in `/etc/snort/snort.conf` Modify the `RULE_PATH`, `SO_RULE_PATH`, and `PREPROC_RULE_PATH` variables to point to your directories in `usr/local/snort`.

You also need to specify an output format. In the config file, look for a line that starts `output unified2` and uncomment that.

Now you can start Snort with the command `/etc/rc.d/snort start`. Log files should be created under `/var/snort`. Next time we will see how we can use those logs.