Lab 10.2 PF Logging
IN715 Networks Administration

September 23, 2015

Introduction

PF can log information about the packets it processes. These logs can be useful when configuring and troubleshooting a firewall. It can also provide information about possible security threats and general network usage. In this lab we will see how to write to and read from PF's logs.

1 Writing to PF logs

To log packets handled by a perticular rule, just add the `log` keyword to that rule as follows:

```
pass log proto tcp from any to any port 22
```

You can also add logging option in parentheses after the `log` keyword.

```
pass log (all, user) proto tcp from any to any port 22
```

The available options are

`all` Causes all matching packets, not just the initial packet, to be logged. Useful for rules that create state.

`to pflogN` Causes all matching packets to be logged to the specified pflog(4) interface. The default log interface is `pflog0`

`user` Causes the UNIX user-id and group-id that owns the socket that the packet is sourced from/destined to (whichever socket is local) to be logged along with the standard log information.

2 Reading the log

PF data is logged to `/var/log/pflog` file. This log is in a binary format that is not human-readable. We use `tcpdump` to view the log.

View the log file with the command

```
tcpdump -n -e -ttt -r /var/log/pflog
```

or you can view logs in real time by reading from the `pflog0` interface

```
tcpdump -n -e -ttt -i pflog0
```

We can use `tcpdump` to restrict its output to show only the data that matches certain conditions. For example,

```
tcpdump -n -e -ttt -r /var/log/pflog port 80
```

shows only packets matching port 80, and

```
tcpdump -n -e -ttt -r /var/log/pflog port 80 and host 192.168.1.40
```

only shows packets matching port 80 on a particular machine. Additional filter options can be found on the `tcpdump` man page of on the OpenBSD PF web pages at `http://www.openbsd.org/faq/pf/`.

3 Experiment with logging

Firewall logs will be an important tool during the upcoming security exercise. Add some logging to your firewall rules and send some sample network traffic so that your logs will have some data in them. Perhaps you should run some port scans. Then inspect your logs to see what information you can get from them.

In real-world scenarios it's important to find a balance between too little and too much logging. You want to caputre relevant information, but you don't want to get buried in logs you'll never read. In the security exercise, however, you should log pretty aggressively.