Published on *Jisc community* (https://community-stg.jisc.ac.uk)

The network monitor

Our monitor is a Linux system running the Snort lightweight intrusion detection system [3] [1]. Demands on hardware are not very high: we use a redundant Pentium 133-based system with two 10/100Mbit/s network interface cards, 128MB memory and 4GB disk space. This allows us to use one interface to access the console, while the other is dedicated to the RSPAN traffic. It is con?gured with a minimum number of services running and no user accounts [4] [2].

Snort is basically a packet sniffer for which a library of network attack signatures is available. It uses signatures in much the same way that most anti-virus software uses them, to recognise patterns in viral code. Snort is not really stateful, and normally analyses packets independently of each other. Preprocessor plugins can be used to extend functionality, for example to detect port scans.

Suspecting that IP spoo? ng might be involved, we want to preserve layer 2 addressing information. This is often critical in identifying the true source of spoofed traffic, as most spoo? ng occurs at layer 3 (IP), rather than at layer 2 (the MAC address). To this end, we can invoke Snort with the following command line options:

[root@monitor [3]]# snort -D -N -e -i eth1 -c ./08292k.rules -l ./logs

The meanings of the options are as follows:

-D	run in background (as a daemon)
-N	do not attempt to log packet payload
-e	record layer 2 information
-i eth1	read packets from interface eth1
-c ./08292k.rules	name of ?le containing attack signatures
-l ./logs	write log ? les to this directory

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/network-monitor

Links

[1] http://www.snort.org/
[2] https://community.ja.net/library/janet-services-documentation/references-3
[3] mailto:root@monitor