IDSs (intrusion detection systems) are applications that detect, log, and alert malicious or suspicious network traffic.

IPSs (intrusion prevention systems) are similar to IDSs but they also prevent suspicious and malicious traffic.

IPSs and IDSs can be either host based or network based.

**How to run Snort**

To run snort for live network monitoring you will need to specify which network port you would like to use snort on with the -i option (example: snort -i eth0)

You will also need to specify rules for snort to abide by.

**How to write and test Snort Rules**

Snort rules can be found in the /etc/snort/rules/local.rules file.

A way to edit this file is the use the command “sudo gedit /etc/snort/rules/local.rules”

Once you are able to edit the file you must know the syntax of snort rules which go as follows

Alert [protocol (ex: tcp)] [source ip] [source port] [direction (-> or <>)] [destination ip] [destination port] (msg:”sample text”; sid:1000001; rev:1;)

Examples



****

**How to analyze alert logs**

To analyze alert logs with snort you can use the -r option to read the a specific pcap.

Ex:snort -r /Desktop/Pcaps/pcap.pcap