IDS/IPS exercise

Jens Schønberg

April 2022

1 Exercise 1. A look at some of the different mechanism

If you haven't then I would recommend to install Wireshark or try a test case with tcpdump to start sniffing and detecting network traffic.

2 Exercise 2. Snort rules

Lets write some simple snort rules

3 Exercise 2. Suricata

Simple suricata setup and listening.

1. install suricata, older system directly from many repo-managers,
2. in newers add the ppa.
3. setup the /etc/suricata/suricata.yaml on newer and restart service
4. older uses oinkmaster and just run suricate on your interface.

the rules are made with an action (alert, drop, pass, reject , ...), a protocol (tcp, udp, http, ssh, dns, smb, ...), a dest/src (direction as well) and a port.

try something like alert tcp $your_address any -¿ $dst_address any (msg:" ... ";flow:established,to_server;)

then add it to some_rule, then add your new rule and path to /etc/suricata/suricata.yaml and run suricata -c /etc/suricata/suricata.yaml -i $interface