FSI LEI 2025/2026

Practical Exercises #4

Goals

Network intrusion detection using Suricata (in Linux)

Materials

- Suricata
- Suricata documentation

Suricata in the packet sniffer mode

1. **Download** and **install** the suricata intrusion detection system with support for the "nfq" DAQ
2. Use suricata as a live packet capture mode to store captured packets (use pcap-logs)
3. Check the contents of pcap files
4. Run suricata in verbose mode.

Suricata as a network intrusion detection system

5. Build a configuration file with rules for suricata/snort applicable to **the following types of communications**:

- Log all ICMP packets detected
- Alert when "POST" commands are detected in HTTP connections

6. Run Suricata inline using the NFQ.