STI MEI/MIEBOM 2022/2023

Practical Exercises #6

Snort in the packet sniffer and logging modes

1. **Download** and **install** the Snort intrusion detection system with support for the "nfq" DAQ.

2. Use Snort as a **packet sniffer** to print all packets (TCP/IP headers and packet contents).

3. Use Snort as a **packet logger** to:

- Log all communications (headers and packet contents) in **ascii** mode.

- Log all IP communications in **binary** mode and next:
    - Use snort in "playback mode" with the logs produced.
    - Use **wireshark** (or **tshark**) to analyze the logs.

Snort as a network intrusion detection system

4. Build a configuration file with rules for Snort applicable to **the following types of communications**:

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

5. Run Snort inline using the NFQ DAQ module. Configure Snort and IPTables to **block all HTTP communications** using the "GET" command.

Goals

Network intrusion detection using Snort (in Linux)

Materials

- SNORT
- SNORT Users Manual 2.9.7
- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, "Capítulo 10. Detecção e prevenção de intrusões"