# Lab Class 6 - Intrusion Detection using Snort

References:

- Snort website
- Snort manual and Documentation
- Snort cheat sheet

## Assignment 1 - Snort initial experiments

1. Install `Snort 2.9` on one of the machines.
2. Try Snort in **packet sniffer mode** (check the snort man page for details on each of the command line option):

   > `snort -v`

3. With application data dumping:

   > `snort -vd -i <interface>` (run this in one machine and then run telnet/ping from another machine into it)

4. In packet logger mode (ascii -- other modes exist):

   > `snort -vd -K ascii -l ./log_folder/`

5. Now ping a machine and check what was logged in the folder "log_folder".

   **Note:** Directories are created according to the source/destination of traffic. Within them, are the files for several protocols/packets.

6. Log in binary (tcpdump) format:

   > `snort -b -l ./log`

7. Snort in "playback mode" from log file:

   > `snort -vd -r snort.log`

8. Reading the packet log file using tcpdump:

   > `tcpdump -r snort.log`

## Assignment 2 - Running Snort as a simple NIDS

1. Create a configuration file (`snort.conf`) to:
   - Log communications using `ICMP``
   - Log and alert when `GET` commands are detected in `HTTP` connections
   - Send all data from previous `HTTP` sessions to a separate log file, in printable (readable) format

- The configuration file can be as follows:

```
log icmp any any -> any any (msg:"Teste";sid:00001;)
```

```
alert tcp any any -> any any (msg:"Um Get!"; content:"GET";
nocase; sid:00002;)
```

```
log tcp any any -> any any
(logto:"myhttpdata";session:printable;sid:00003;)
```

Check the meaning of these configurations and how to write rules in the Snort manual and Documentation.

2. To avoid interference from other traffic test locally (i.e., using the `loopback` interface) with:

```
snort -vd -l ./snort_log/ -c snort.conf -K ascii -k none -i lo
```

3. Now ping your own machine and access a local webserver (may need to install and start it):

    - ```
      ping 127.0.0.1
      ```
    - ```
      telnet 127.0.0.1 80
      ```
    - ```
      GET /
      ```

4. Check files `snort_log/alert` and `snort_log/myhttpdata` and also within folder `127.0.0.1`.

5. Investigate how to use Snort to **detect port scanning** (e.g., `nmap`):

    - Check the following documentation on `sfportscan`
    - Register and download `snortrules-snapshot-29111` (https://www.snort.org/downloads#rules)
    - Using the configuration file for Snort (usually under `/etc/snort/snort.conf`) and the community rules for your Snort version (that you can also put in `/etc/snort/`), set Snort to detect port scanning attempts (e.g., with `nmap`) to the local system.
    - Run Snort in NIDS mode
    - Launch a port scan (e.g. `UDP` port scan with `nmap`) to the system, and check if it was detected in the log files

- Investigate other attacks that can be detected by Snort by configuring rules to testing them accordingly.

Naturally, there are more user-friendly dashboards to keep track of Snort events. For example: in a Grafana Snort IDS/IPS Dashboard

---
      ```