Network Intrusion Detection and Prevention – assignment no. 1

- **Task 1:**
  - Set home network to IP address of your virtual machine.
  - Install freely available "Emerging threats Open (ET Open)" rules.
  - Start suricata as a service in IDS mode.
  - Demonstrate correct functionality of rules by generating a test alert.
- Number of points: 0.5

Network Intrusion Detection and Prevention – assignment no. 2

- **Task 1:**
  - Create a rule that alerts on connection attempts from your VM to a specific IP address and TCP port.
- **Task 2:**
  - Create a rule that alerts on HTTP connection attempts from your VM in direction to server using non-standard ports.
  - Use automatic protocol detection.
- Test the configuration and demonstrate correct function of the rules in IDS mode.
- Explain the reasoning behind monitoring outgoing communication from the monitored network.
- Number of points: 1 pt.

Network Intrusion Detection and Prevention – assignment no. 2 (cont.)

- **Task 3:**
  - Run the shell from the previous Lab on a selected port and connect to it from another (colleague's) machine.
  - Create a rule that drops packets that contain a string "/etc/shadow" in established connection on the selected port in direction to server.
  - Test the configuration and demonstrate correct function of the rule in L3 inline IPS mode.
- Number of points: 0.5 pt.

Notes

- Save your own rules to file */var/lib/suricata/rules/local.rules*.
- Test the rules from another machine (e.g. colleague's) – traffic with the same source and destination IP may be considered suspicious.
- In case snort does not correctly detect sessions, there could be an issue with incorrect packet checksums – use option -k.
- Edit firewall rules if needed.
- Use program netcat or python to simulate listening services.

References

- man suricata
- https://suricata.readthedocs.io/en/suricata-6.0.8/rules/index.html
- https://suricata.readthedocs.io/en/suricata-6.0.8/rule-management/index.html
- https://suricata.readthedocs.io/en/suricata-6.0.8/setting-up-ipsinline-for-linux.html
- man iptables
- man nc
- https://docs.python.org/3/library/http.server.html