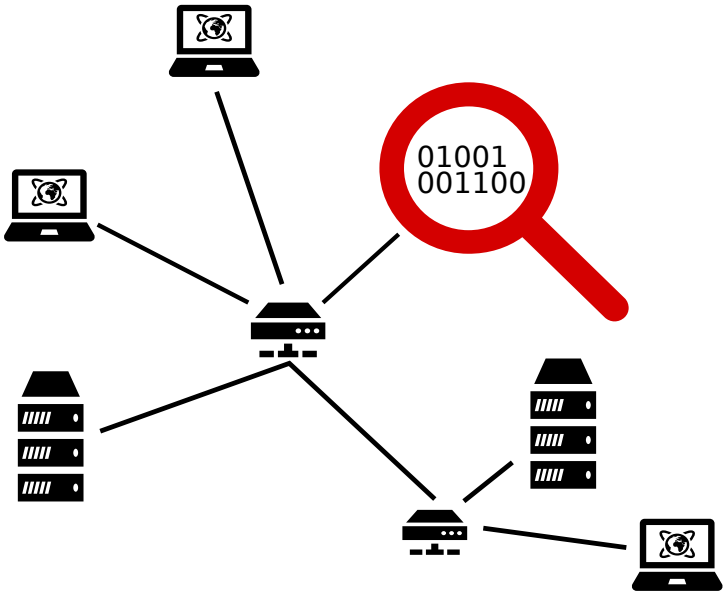
PADERBORN UNIVERSITY
Prof. Dr. Falko Dressler
Distributed Embedded Systems – CCS Labs
CCS

Bachelor Thesis

Distributing the Load of Signature Based NIDS

Signature-based Network Intrusion Detection Systems (NIDS) are the state-of-the-art when it comes to precise attack detection and intrusion prevention. Using well-defined signatures allows for precise attack descriptions to detect known intrusions and vulnerabilities in network traffic. However, the accuracy of these systems comes at the cost of critical performance problems in modern high-speed networks [1]. These performance problems may lead to packet drops and, thus, to undetected events.



Tasks

In this thesis, the student evaluates different strategies to distribute the load of a signature-based NIDS to multiple machines. Snort [2] is the most widely used signature-based NIDS and provides the biggest database of signatures, thus, will use Snort as the NIDS of choice in this thesis.

The main goal of the thesis is to reduce the dropped packets as much as possible while retaining a high detection rate. The proposed solutions have to be confirmed with an extensive experiment campaign using realistic traffic [3], [4]. The following questions should be answered during this thesis:

- Is it better to distribute signatures or traffic on multiple machines?
- What are the criteria of distribution for the signatures/traffic?
- What is the influence of different traffic patterns/characteristics on the distribution strategy?

Required skills (or willing to learn)

- Networking basics
- Basic knowledge about the Snort NIDS

Keywords

Network Security, Intrusion Detection, Snort, Linux, iptables

[1] F. Erlacher and F. Dressler, "FIXIDS: A High-Speed Signature-based Flow Intrusion Detection System," in *IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*, Taipei, Taiwan: IEEE, Apr. 2018. DOI: 10.1109/NOMS.2018.8406247.

[2] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," in *13th USENIX Conference on System Administration (LISA 1999)*, Seattle, WA, Nov. 1999, pp. 229–238.

[3] F. Erlacher and F. Dressler, "How to Test an IDS? GENESIDS: An Automated System for Generating Attack Traffic," in *ACM SIGCOMM 2018, Workshop on Traffic Measurements for Cybersecurity (WTMC 2018)*, Budapest, Hungary: ACM, Aug. 2018, pp. 46–51. DOI: 10.1145/3229598.3229601.

[4] ——, "Testing IDS using GENESIDS: Realistic Mixed Traffic Generation for IDS Evaluation," in *ACM SIGCOMM 2018, Demo Session*, Budapest, Hungary: ACM, Aug. 2018, pp. 153–155. DOI: 10.1145/3234200.3234204.

Contact:
Felix Erlacher <erlacher@ccs-labs.org>

Website:
http://www.ccs-labs.org