Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

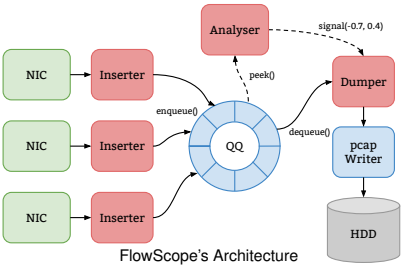
Thesis B.Sc.

IDP

Detection and Analysis of Security Incidents in Honeypots using FlowScope

Motivation

Honeyed networks (honeypots) are means for intrusion detection deployed in the public Internet. Existing in various architecutes, all types of honeypots simulate legitimate network resources (e.g. emulating a mail/web server) with some open standard ports. The main purpose is then to detect and study attacker behavior and intrusive characteristics by monitoring the traffic that enters them.



FlowScope's Architecture

This thesis aims to detect security incidents using live data from honeypots and evaluating them. For that reason we exploit FlowScope, a digital storage oscilloscope developed by the Chair of Network architectures and Services at TUM [1]. It is an oscilloscope that is able to capture traffic from high speed links (up to 120 Gbit/s) continuously in a ring buffer data structure in memory. A desired portion of the traffic can then be dumped to disk using a dedicated filter on trigger events. The stored traffic can subsequently be further analyzed.

The goal of this thesis is, hence, to deploy FlowScope in a real network with appropriate filter rules based on the live input data provided from a honeypot. The suspicious traffic is then captured, analyzed, and persisted in a systematic way.

Your Task

- Deploy means to automatically capture live data from the honeypot
- Extract relevant rules to determine intrusive traffic elements from the data
- Exploit FlowScope's REST API to feed in the rules and capture intrusive traffic (if existent) in a real network
- Evaluate intrusive traffic, attacker behavior, etc.

Contact

Paul Maximilian Emmerich emmericp@net.in.tum.de
Minoo Rouhi rouhi@net.in.tum.de
Dominik Scholz scholz@net.in.tum.de

[1] https://github.com/emmericp/FlowScope