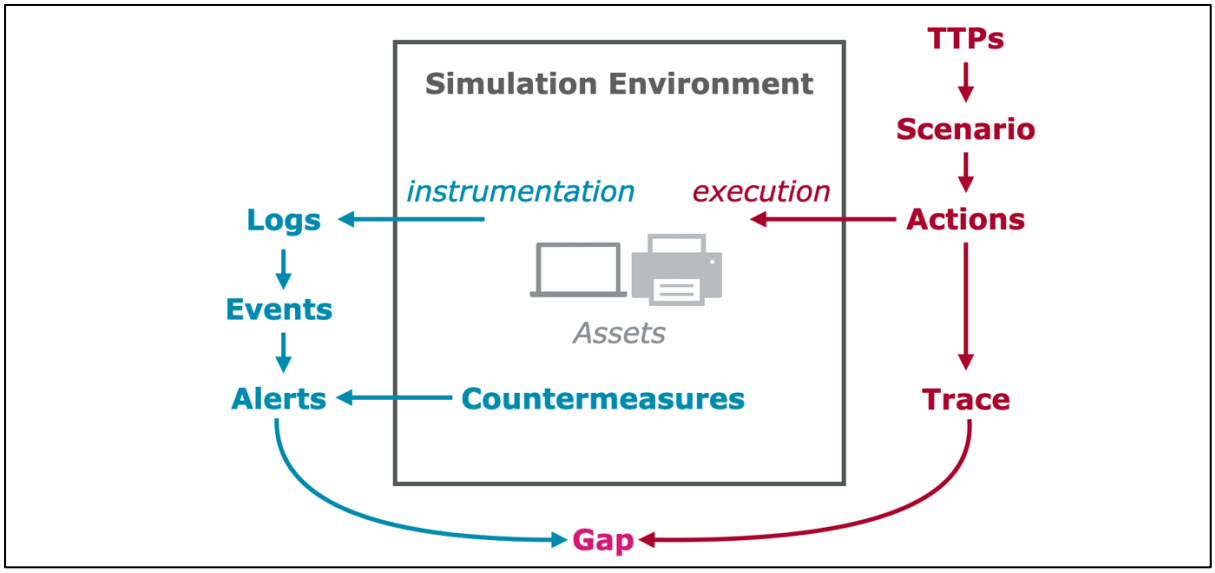
Prof. Dr. Christoph Meinel
IT Security Engineering (Sec-Eng) Team
Internet Technologies and Systems Group

Towards Automated Red Team Exercising
- Proposal for a Master Project in WS2022/23

Background

Nowadays, more and more organizations start to use red teaming exercises to simulate attacks or threats against their IT operations for testing and improving their defense posture. While pen testing is a structured approach using an enumeration of attacks, red teams assume the identity of a factious threat actor with its individual intent and skill level. These threat fictional are often based on real adversaries and mimic their tactics, techniques, and procedures (TTPs). Public databases like MITRE ATT&CK provide an enumeration of TTPs belonging to a certain advanced persistent threat and provide planning guidance.



Objectives

As red teaming is a highly creative and risky process, a full automation of exercises is not feasible. It is anyways a repetitive process as many organizations aim for continuous verification of new defenses and red-teamers test scenarios in different environments.

The goals of this master project will be to

(1) propose and implement a tool to assist a human with the creation, risk assessment, execution, evaluation, and reporting of an adversary emulation;

(2) showcase a few sample exercises using the tool.

Some questions we'd like to answer with this project are (but not limited to):

- How to automate the design and risk evaluation of an adversary emulation?
- What are useful metrics to measure the success of an exercise?
- How to map detections and countermeasures to red-teaming actions?
- How to manage (execute, monitor, visualize, and assess) the exercise as well as the identified defensive gaps?

Deliverables

The deliverables of this project include:

- Design and PoC implementation of a semi-automated red teaming toolkit
- 2-3 read teaming exercises based on the proposed toolkit
- a technical report

Target Disciplines (sorted by priorities)

- **Cybersecurity**
- IT-Systems Engineering
- Data Engineering

Contacts

Wenzel Pünter, Pejman Najafi, Dr. Feng Cheng, Prof. Dr. Christoph Meinel
Email: security-analytics@hpi.de | Room: H-1.10/12 | Tel: +331-5509-519