RI CODE
Research Institute
Cyber Defence
Universität der Bundeswehr München

Towards a Concept for Actionable Documentation for Cyber-Range Scenarios (Several MAs possible)

Prüfer: PD Dr. Corinna Schmitt (UniBw M / LMU)

Betreuung: Christoph Steininger (UniBw M)
Matthias Schopp (UniBw M)

Kontakt: christoph.steininger@unibw.de
matthias.schopp@unibw.de

Bei Interesse bitte grundsätzlich alle Betreuer informieren (Nutzung von CC)

- Motivation and Tasks -

The rising frequency of cyber attacks has underscored the critical need for comprehensive cyber security training across various sectors, including companies and government agencies. For example, the Federal Office for Information Security (BSI) in Germany publishes the yearly report "Die Lage der IT-Sicherheit in Deutschland", shedding light on the current state of IT security and emphasizing the need of effective training [1]. One effective method for conducting cyber security training is through the use of Cyber-Ranges, specialized environments that allow to conduct realistic training for security incidents without compromising productive infrastructure. However, the creation of such training scenarios is a complex and expensive task that demands highly specialized knowledge.

To ensure the success of cyber security training programs, it is crucial that all personnel involved deeply understand the procedures and milestones of each training scenario. This includes not only those responsible for building scenarios but also individuals involved in training execution, such as instructors and debriefing personnel. Therefore, easily comprehensible documentation is key - for trainers, but also for trainee-debriefing or potential scenario sharing between Cyber-Ranges. Teaching and learning processes can benefit from using tools that combine different types of resources as text, images or executable code [2]. Drawing inspiration from tools like Jupyter notebooks in data science, the thesis aims to create a concept for actionable documentation that can be universally adopted by different cyber-range platforms. 'Actionable documentation' is thereby refer-

[1] `https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html`, abgerufen am 12.02.2024

[2] Al. Cardoso, J. Leitão, C. Teixeira: Using the Jupyter Notebook as a Tool to Support the Teaching and Learning Processes in Engineering Courses. In ICL 2018: The Challenges of the Digital Transformation in Education pp 227–236.

red to as a combination of executable code and continuous text that succinctly describes its function and can be used for learning as well as facilitating scenario orchestration within a Cyber-Range.

In the context of this thesis a concept for actionable documentation for Cyber-Range scenarios is to be developed. The focus is to develop an open approach that can be adopted by different Cyber-Range platforms. The scope is to describe a team-training scenario, wherein the trainers' side undertakes defensive/offensive actions in a simulated cyber-incident scenario, and trainees are required to respond effectively according to the training's mission. The concept developed in this thesis will be evaluated through a proof of concept implementation. This implementation will involve the execution of a cyber-attack within a small, simulated network in a Cyber-Range environment.

Key Areas:

- Development of a documentation guideline for Cyber-Range red/blue team scenarios based on cyber attack workflows
- Requirements analysis for orchestrating a training scenario in a fully virtualized Cyber-Range using freely available software
- Integration of the documentation guideline with the orchestration of the training scenario into a generic concept for actionable documentation for Cyber-Ranges, which can be implemented on top of an existing Cyber-Range
- Demonstration of the viability of the concept through implementation in a self-developed Cyber-Range red/blue team training scenario

Start Literature:

- Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636.
- Cardoso, A., Leitão, J., & Teixeira, C. (2019). Using the Jupyter notebook as a tool to support the teaching and learning processes in engineering courses. In The Challenges of the Digital Transformation in Education: Proceedings of the 21st International Conference on Interactive Collaborative Learning (ICL2018)-Volume 2 (pp. 227-236). Springer International Publishing.
- Mayer, R. E. (2003). The promise of multimedia learning: using the same instructional design methods across different media. Learning and instruction, 13(2), 125-139.