Master Project SoSe 2022

A Cyber Range for Hands-On Security Exercises and CTFs

FG Cybersecurity and Enterprise Security, Prof. Dr. Christian Dörr

Background

Obtaining hands-on practice with computer networks is difficult. Most people do not own multiple, spare computers to setup a scenario at home, while on campus resource-intensive, large-scale exercises can only be provided for a short time and not on demand. This is especially true when it comes to security-related exercises, where part of the assignment — and the excitement — is to experience what happens when things go wrong.

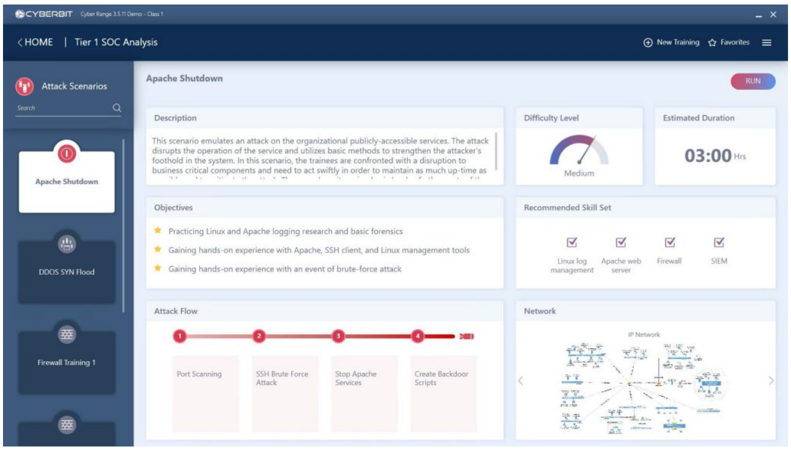
The goal of this project is to build a so-called "cyber range", an environment where each student can create and operate a large-scale realistic network, and experiment with it in a protected environment. We plan to use this cyber range in the upcoming semester(s) to realize hands-on components to the new network security courses, so that students can gain first hand experience how cyber attacks work and how to defend against them.

Project Goal

There exists already a proof-of-concept that demonstrated the possibility to dynamically spin up and configure a set of virtual machine based on a machine-readable configuration file, and make VM topologies available via a personalized VPN entry point.

The aim of this project is to turn this PoC into a deployable cyber range learning environment, where students can select scenarios to play from a scenario library in a cyber range dashboard (for an example see on the right), with the system commissioning the environ-ment either on local servers or instances leased from cloud providers.

To allow for more interaction, individual exercises can be played in a red team/blue team configuration, and it should be possible to connect physical hardware (such as IoT sensors) into the simulated topology.



This scenario emulates an attack on the organizational publicly-accessible services. The attack disrupts the operation of the service and utilizes basic methods to strengthen the attacker's foothold in the system. In this scenario, the trainees are confronted with a disruption to business critical components and need to act swiftly in order to maintain as much up-time as

- Practicing Linux and Apache logging research and basic forensics
- Gaining hands-on experience with Apache, SSH client, and Linux management tools
- Gaining hands-on experience with an event of brute-force attack

Image: CyberBit Range

Contact Information

Prof. Dr. Christian Dörr	christian.doerr@hpi.de	Haus III, G-3.1.09