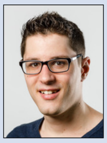
Sinthujan
LOHANATHA
N



Severin
Marti

Live Response Training Range mit Velociraptor

Logo Velociraptor
https://www.velocidex.com/images/logos/logo.svg

Logo Hacking-Lab
https://hsr.hacking-lab.com/events

Initial Situation: With the ever-increasing number of cybersecurity incidents happening world-wide, incident response is becoming a central part of any cybersecurity education training. In response to this, OST is offering a new CAS course named Cyber Security. One recently becoming popular tool for incident response is Velociraptor. The goal of this project was to create training material for students covering incident response practices using Velociraptor and Volatility. Moreover, to simulate a realistic attack scenario, a compromised training range based on Microsoft Azure needed to be provided.

Approach / Technology: For that purpose, a training range designed for offensive security attack scenarios was tailored to suite the needs for the incident response exercises. As was the case with the provided training range, deployment of the new environment is done with Terraform. The virtual machines and Active Directory domain from the existing offensive security training range were largely kept and built upon. New exercises – called challenges – were implemented by adding to existing or adding new Terraform code, PowerShell or Python scripts. To facilitate coordinating the simulated attack, a C++ server-client application was developed to simulate the attacker.

Result: In total, 11 challenges were implemented. The challenges are formatted to be included in OST's Hacking-Lab and cover Velociraptor deployment and the forensic analysis of initial access, multiple persistence mechanisms, lateral movement, and privilege escalation. Additionally, students will learn how to perform memory analysis with Volatility and Velociraptor, squid proxy log parsing, and how to clean an infected environment after an attack (eradication). The challenges are designed and ordered in such a way as to guide the students through investigating the cybersecurity incident. Additional challenges can easily be implemented building on the existing environment to simulate additional attack techniques or incident response steps.