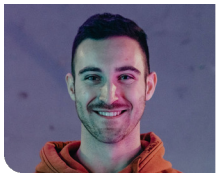
MISP - Malware Information Sharing Platform

Studenten

Marius Zindel



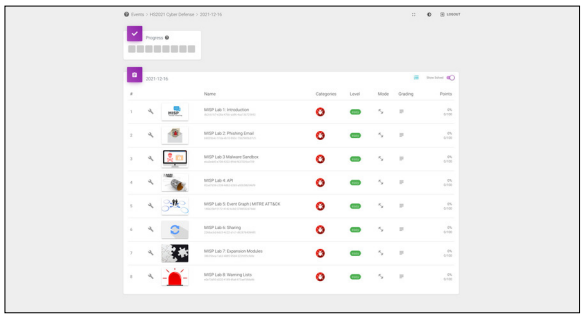
Janis Wolf

Problemstellung: Das Cyber Defense Modul an der OST vermittelt Studierenden diverse Tools und Methoden, um sich besser gegen Cyber Kriminelle zu schützen. Dazu gehört auch MISP (Malware Information Sharing Platform), eine Software für die Klassifizierung und den Austausch von Indicators of Compromize (IOCs) und Malware Samples.

Ziel der Arbeit: Ziel dieser Arbeit ist die Erstellung von 8 verschiedenen Laborumgebungen auf der Hacking-Lab Plattform, um den Studierenden einen Einblick in MISP zu geben. Ein Lab beinhaltet jeweils eine Einführung ins Thema, eine Problemstellung mit Step by Step Anleitungen, sowie Verständnisfragen und eine Lernkontrolle.

Ergebnis: Es wurden 8 unterschiedliche MISP-Labs erstellt. Sie behandeln diverse Features von MISP und decken einen grossen Teil der MISP-Funktionalität ab. Auf GitHub wurde ein Repository eingerichtet, welches die MISP installation auf Basis von Docker automatisiert. Die Docker Labs sind modular und können einfach via Skript (Python) angepasst werden. Die Übungen sind auf die Hacking-Lab LiveCD https://livecd.hacking-lab.com/ abgestimmt.

Übersicht Hacking Lab (alle 8 Übungen)
Eigene Darstellung



Examinator
Ivan Bütler

Experte
Bütler Ivan, Rapperswil-Jona, SG

Themengebiet
Networks, Security & Cloud Infrastructure, Sicherheit