

Open Source Intelligence Training in Hacking-Lab

Graduate

Damian Dasser

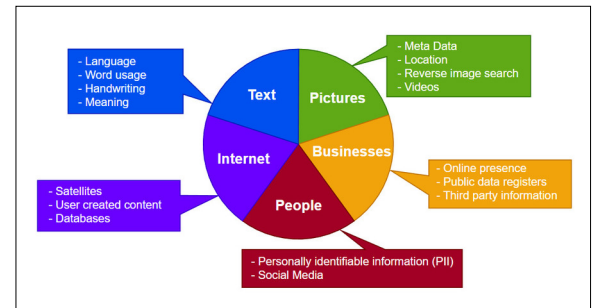
Initial Situation: In cyber security the topic of Open-source intelligence (OSINT) plays a major role. With OSINT security defender and researcher may find valuable information about cyber crime and attackers. OSINT helps to understand the effects of sharing public information. OSINT is not yet part of the curriculum at OST. An e-learning platform called Hacking-Lab already exists and is used at OST. In Hacking-Lab, students can apply what they have learned in the lecture in a controlled environment in the form of practical hands-on exercises.

Objective: The goal of this thesis was to create 10 OSINT challenges in the Hacking-Lab for students to solve and practice. In every OSINT challenge, students are given a set of tasks and summative assessment questions. The students are guided through the proposed steps in order to answer the posed questions in form of a write-up. Each OSINT challenge is framed by a story to make them more engaging. These stories were chosen in a way that many different OSINT techniques are applicable and can be practiced by the students. In OSINT there is not only one way to find the correct answer hence the students are also encouraged to find their own way to reach the expected solution. To guarantee a high quality of the challenges, multiple quality assurance tests were conducted with students and colleagues working in IT. The results of these quality tests are an indicator whether the goal was reached.

Result: As a result of this work, the goal of creating ten OSINT challenges in Hacking-Lab was achieved. These challenges provide some insight into the topic of OSINT without getting lost in details and technicalities. This project provides a foundation which a lecturer can build upon by creating a lecture on OSINT. This lecture could be integrated in a

course on cyber security. Social media was purposely neglected in this project because social media is difficult to maintain and make future-proof, which makes it incompatible with the project's requirements. Therefore, it could also be a future project to expand upon these challenges with a focus on social media as it is an indispensable part of OSINT.





















OSINT categories used in this thesis
Own presentation



Challenge example: What did the sign this CCTV camera is mounted on say in 2018?
Center Harbor Inn



The created challenges in the Hacking-Lab
Hacking-Lab AG

#	Name	Categories	Level	#	Name	Categories	Level
1	 01 - Scamming Personal Information b39b6263-141a-4f0d-8927-30201f005959		easy	6	 06 - Show What You Have Learned 69d55549-87ad-40fa-4b2a-08bee8fddd2		medium
2	 02 - The Propagandist's Information 825a00bc-5474-40d2-ad34-9c0d3225c829		medium	7	 07 - Vulnerability Information 45432888-540b-49be-8a84-2b4873490c76		novice
3	 03 - Time for Waste 00dc1eea-5b05-4e0c-ad34-9c0d3225c845e		easy	8	 08 - Run After Ransomware 3306164a-5b4e-4ce6-b1fc-79d2998e9d95		medium
4	 04 - Validate Internet Post 88dfdb5c-aaa5-4c2c-84f6-8985dcb07bfa		easy	9	 09 - A Car's History 65033668-4b98-4b22-b790-1db8eebf6a7e		novice
5	 05 - Third Party Software Contributions 8be49b45-5afe-490c-9477-5bb6808763a7		easy	10	 10 - Malicious Gamer 73e9cb77-1ff4-43c4-883f-3141d8e9e0d8		easy

Advisor
Ivan Bütler

Co-Examiner
Vanessa Procacci,
Kantonspolizei Aargau
/IT-Forensik &
Cybercrime IFC,
Rupperswil, AG

Subject Area
Security