Entwicklung IT Forensik CTF Workshop für ICT Lernende

Studiengang: MAS Cyber Security

Gamification im Unterricht wendet der Autor schon seit Jahren als Kursleiter in der Berufsbildung und Erwachsenenbildung an und ist immer auf der Suche nach neuen und alternativen Ausbildungsmethodiken. Im Rahmen dieser MAS Thesis wurde ein CTF (Capture the Flag) Workshop zum Thema IT Forensik für die jugendliche Zielgruppe der Informatiklernenden konzipiert und durchgeführt.

David Hügli

Einleitung

Der Autor arbeitet seit Jahren nebst seiner Haupttätigkeit als Linux Engineer als Kursleiter in der Berufsbildung und Erwachsenenbildung. In dieser Zeit hat er viele verschiedene Methoden zur Wissensvermittlung kennengelernt und angewendet. In diesem Studium an der BFH hat der Autor im CAS SIM im eintägigen «Capture the Flag» (CTF) Workshop mit MELANI und CSIRT des BIT's eine weitere Lernmethode entdeckt. Diese Methode möchte der Autor mit dieser MAS Thesis besser kennenlernen, da es ihn selbst in den Bann gezogen hat und er sich die Frage gestellt hat, ob dies auch für Jugendliche in der ICT Ausbildung geeignet ist. Um den Workshop durchführen zu können, konnte der Autor auf ein grosses persönliches Netzwerk zurückgreifen und die Lernenden Ausbildung der Führungsunterstützungsbasis der Armee (FUB) in Bern mit der Idee gewinnen.
Folgende Fragestellung möchte der Autor mit dieser Arbeit beantworten:
- Ist es möglich ICT Lernende der FUB für die IT-Forensik zu begeistern?
- Ist die CTF Methode für die ICT Lernenden der FUB geeignet?
- Ist es möglich in einem Workshop von 4-5 Tagen die Grundlagen der IT-Forensik an ICT Lernende der FUB zu vermitteln?

Umsetzung

Im Rahmen dieser Arbeit wurde zuerst eine Stakeholder Analyse bei den Lernenden der FUB wie auch beim Berufsbildungsverantwortlichen mit dem Ziel durchgeführt, eine Übersicht der demografischen Daten, der Lernsituation, der Vorkenntnisse und den Wünschen zu bekommen. Auf Grund deren Ergebnisse konnten die Grob und Feinlernziele für den Workshop definiert werden. Nebst den Fachthemen der Logfile Analyse und Disk-, Netzwerk-, und Malware/Memory Forensik waren Themen zur Sensibilisierung des Themas gewünscht. In der Planung des Workshops wurde dies mit den Themen Forensik, Ethik und Recht berücksichtigt.

Durch die Definition der Lernziele konnte die Feinplanung der 5 Workshop Tage und das didaktische Konzept mit der Implementation der CTF Methodik erstellt werden. Vorgesehen ist jeweils zu Tagesbeginn ein theoretischer Block, um die notwendigen Methodiken und Tools zur Forensik vorzustellen. Vormittags ist jeweils zum Vertiefen der Theorie eine Einzel Challenge geplant, in der im Prinzip jede/r gegen jede/n spielt. Nachmittags ist ein Team Contest zum jeweiligen Thema vorgesehen.
In der Realisation wurden die Logfiles und Netzwerk Streams in einer virtuellen Umgebung erstellt und den Teilnehmern zur Verfügung gestellt. Bei der Memory/Malware Thematik wurde auf vorhandene Images der Community zurückgegriffen.
Im Rahmen dieser Arbeit wurde auch ein Bash Skript mit MariaDB Anbindung konzipiert und umgesetzt, damit die Teilnehmer die Antworten selbständig prüfen können.

Ergebnis

Der Workshop konnte in der ersten Januarwoche 22 wie geplant durchgeführt werden, jedoch Corona bedingt online statt vor Ort. Somit konnten die gruppendynamischen Prozesse in der Schlussanalyse etwas weniger interpretiert werden.
Die Evaluationen des Workshops bei den Teilnehmern haben gezeigt, dass es möglich ist, ICT Lernende bei der FUB für die IT-Forensik zu begeistern und in einem Workshop von 5 Tagen die Grundlagen der IT-Forensik an junge Berufsleute zu vermitteln und sie dafür zu sensibilisieren.
Etwas differenzierter ist die Meinung der Teilnehmer über Eignung der Methodik, einerseits Begeisterung, anderseits ist der Konkurrenzdruck gerade bei den schwächeren Teilnehmern der Einzel Challenges nicht zu vernachlässigen. Dies wurde durch den Workshopleiter schon nach dem ersten Tag bemerkt und konnte dank dem flexiblen Konzept und der entsprechenden Umsetzung im Tool selbst kurzfristig umgeplant werden.