An Empirical survey of functions and configurations of open-source capture the Flag (CTF) environments

Stela Kucek, Maria Leitner

PII: S1084-8045(19)30330-3

DOI: https://doi.org/10.1016/j.jnca.2019.102470

Reference: YJNCA 102470

To appear in: *Journal of Network and Computer Applications*

Received Date: 18 February 2019

Revised Date: 8 August 2019

Accepted Date: 20 October 2019

Please cite this article as: Kucek, S., Leitner, M., An Empirical survey of functions and configurations of open-source capture the Flag (CTF) environments, *Journal of Network and Computer Applications* (2019), doi: https://doi.org/10.1016/j.jnca.2019.102470.

An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments

Stela Kucek[a], Maria Leitner[a,*]

[a]*AIT Austrian Institute of Technology, Center for Digital Safety & Security, Giefinggasse 4, 1210 Vienna, Austria*

Abstract

Capture the Flag (CTF) is a computer security competition that is generally used to give participants experience in securing (virutal) machines and responding to cyber attacks. CTF contests have been getting larger and are receiving many participants every year (e.g., DEFCON, NYU-CSAW). CTF competitions are typically hosted in virtual environments, specifically set up to fulfill the goals and scenarios of the CTF. This article investigates the underlying infrastructures and CTF environments, specifically open-source CTF environments. A systematic review is conducted to assess functionality and game configuration in CTF environments where the source code is available on the web (i.e., open-source software). In particular, from out of 28 CTF platforms, we found 12 open-source CTF environments. As four platforms were not installable for several reasons, we finally examined 8 open-source CTF environments (*PicoCTF, FacebookCTF, HackTheArch, WrathCTF, Pedagogic-CTF, RootTheBox, CTFd and Mellivora*) regarding their features and functions for hosting CTFs (e.g., scoring, statistics or supported challenge types) and providing game configurations (e.g., multiple flags, points, hint penalities). Surprisingly, while many platforms provide similar base functionality, game configurations between the platforms varied strongly. For example, hint penalty, time frames for solving challenges, limited number of attempts or dependencies between challenges are game options that might be relevant for potential CTF organizers and for choosing a technology. This article contributes to the general understanding of CTF software configurations and technology design and implementation. Potential CTF organizers and participants may use this as a reference for challenge configurations and technology utilization. Based on our analysis, we would like to further review also commercial and other platforms in order to establish a golden standard for CTF environments and further contribute to the better understanding of CTF design and development.

Keywords: CTF, capture the flag, cyber range, computer network operations, cyber security exercises, cyber security training

1. Introduction

Capture the Flag (CTF) is a challenge-based competition for gaining and training cyber security related skills by actively applying them. In a CTF, a team (or a single player) solves problems related to cyber security, and if their answer (also often referred to as flag or solution) to the problem is correct, they get rewarded with points. The aim is to score more points than other participants, which contributes to the competition. CTF platforms (also often referred to as CTF environments or CTF frameworks in literature) are typically used as game-like environments where participants may practice computer security abilities, skills and knowledge. Various attack techniques or skills can be tested such as (e.g., [1, 2, 3]). Long-term goals of CTF competitions e.g., in education would be to allow participants to test computer security skills and abilities, enhance hands-on experience and challenge and test the participants (see e.g., [4, 5]). A more elaborate definition of CTFs and other terms can be found in Section 2.1.

In the past years, many CTF competitions have been conducted and attracted many participants

*Corresponding author.
Email addresses: stela.kucek.fl@ait.ac.at (Stela Kucek), maria.leitner@ait.ac.at (Maria Leitner)