Introduction to useful concepts for solving challenges in "Miscellaneous" category in UniWA-CTF

Michael Kokkos, Alexander Soloviev

Athens, Greece

Abstract

CTF competitions include various challenge categories. But, sometimes, there are challenges that do not fit in any of the predefined categories, or they fit in more than one, these challenges are included into a special category, which is called "Miscellaneous". UniWA-CTF introduces its participants to the fields of Esoteric programming languages and dictionary attacks by providing one challenge for each field in this specific category. The purpose of this paper is to assist the users with theoretical knowledge, so that they can help themselves solve the challenges and build a foundation of knowledge in these topics.

Keywords: CTF, Miscellaneous, Esoteric Programming Languages, Dictionary Attacks

1. Introduction

This paper provides its readers with foundational knowledge about two unrelated subjects that the participants of UniWA-CTF competition will meet in the "Miscellaneous" challenge category.

The first topic of the paper is Esoteric Programming Languages, also known as "esolangs". Esolangs are being widely used in CTF competitions as parts of some challenges or even as stand-alone challenges. Although they are not directly related to cybersecurity, they can be a fun way to puzzle and challenge the problem solving capabilities of the participants.

The second topic of the paper is dictionary attacks. A dictionary attack is a form of brute force attack. These types of attacks are usually used in CTF competitions as a step for solving a bigger challenge (e.g. accessing a website admin's interface or a password protected file).

Preprint submitted to University Of West Attica *March 17, 2021*

2. Esoteric Programming Languages

Esolangs are a practice of hacker/hobbyists, with most of them being experimental works. Esolangs are a subversive practice within computer science that take the design of a programming language to places far outside of practical utility. That happens by postulating various what-if scenarios and then designing a programming language around them [1].

Esolangs are experimenting with weird ideas, like being hard to program in, minimalism, brevity, obfuscation, or even as a joke. There is a small but active Internet community of people creating esolangs and writing programs in them, as well as debating their computational properties (e.g. if said languages are Turing-complete).[2]

2.1. Examples of Esolangs

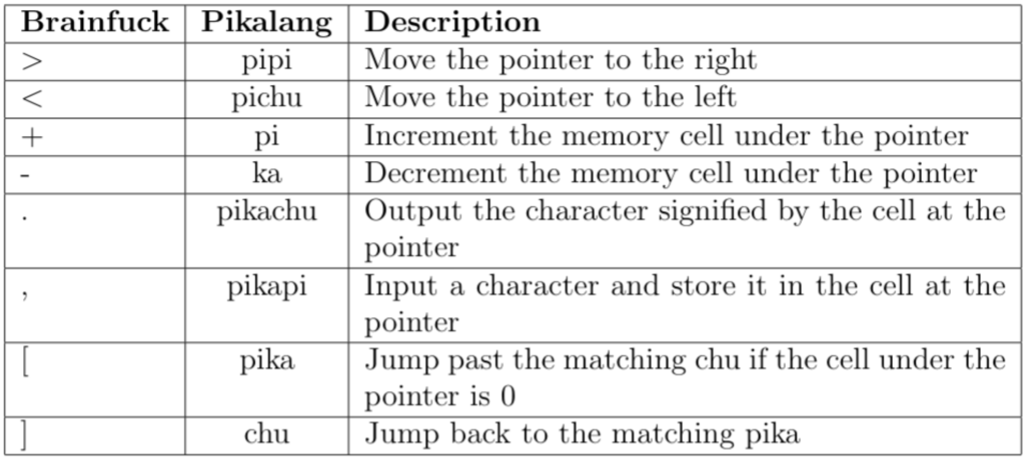
Although its small size, the community has developed a lot of esolangs. It is not the purpose of this paper to document all these languages, this section includes two of them that they are somehow relatable with the UniWA-CTF competition.

2.1.1. Brainfuck

Brainfuck is an esolang created in 1993 by Urban Müller [3]. Müller designed Brainfuck with the goal of implementing it with the smallest possible compiler[4], it uses eight language commands, each one consists of only a single character, these commands are explained in the next subsection, along with their Pikalang corresponding commands. This paper does not dive deep into the technical details of programming in Brainfuck, as there are multiple online sources dedicated to do that in detail. If someone wants just to encode or decode a Brainfuck program, he or she can do that easily without extensive knowledge just by querrying a search engine for an online encoder/decoder for that purpose.

2.1.2. Pikalang

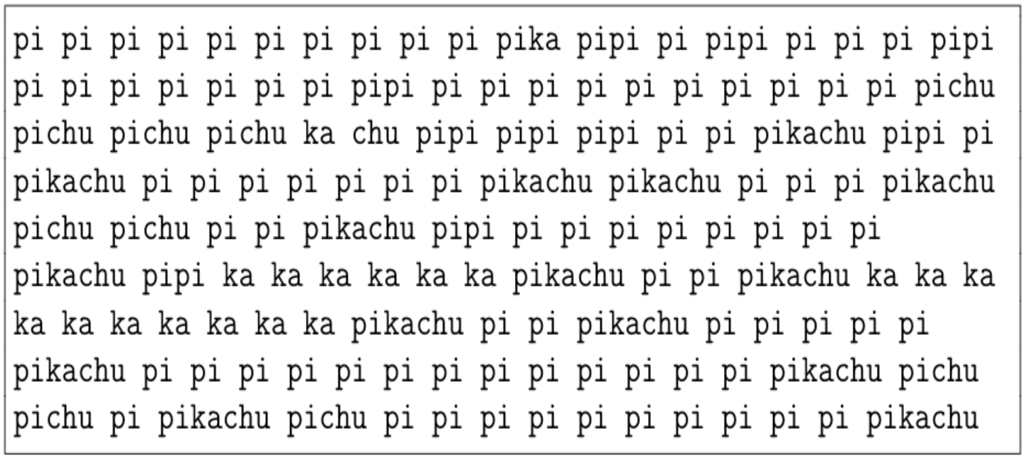
Pikalang is a brainfuck derivative based off the vocabulary of Pikachu from the Pokémon video game series, created by Blake Grotewold [5], [6]. It is identical to Brainfuck, except that the instructions are changed into the sounds made by Pikachu from Pokémon [5].



Brainfuck	Pikalang	Description
>	pipi	Move the pointer to the right
<	pichu	Move the pointer to the left
+	pi	Increment the memory cell under the pointer
-	ka	Decrement the memory cell under the pointer
.	pikachu	Output the character signified by the cell at the pointer
,	pikapi	Input a character and store it in the cell at the pointer
[	pika	Jump past the matching chu if the cell under the pointer is 0
]	chu	Jump back to the matching pika

Figure 1: Corresponding pikalang commands to these of brainfuck

Figure 2, shows the famous ”Hello World” program written in Pikalang, printing the phrase ”Hello Pikachu!”.



```
pi pi pi pi pi pi pi pi pi pi pika pipi pi pipi pi pi pi pipi
pi pi pi pi pi pi pi pipi pi pi pi pi pi pi pi pi pi pi pichu
pichu pichu pichu ka chu pipi pipi pipi pi pi pikachu pipi pi
pikachu pi pi pi pi pi pi pi pikachu pikachu pi pi pi pikachu
pichu pichu pi pi pikachu pipi pi pi pi pi pi pi pi pi
pikachu pipi ka ka ka ka ka ka pikachu pi pi pikachu ka ka ka
ka ka ka ka ka ka ka pikachu pi pi pikachu pi pi pi pi pi
pikachu pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu pichu
pichu pi pikachu pichu pi pi pi pi pi pi pi pi pi pi pikachu
```

Figure 2: Hello World type program in Pikalang

3. Dictionary Attacks

A dictionary attack is a form of brute-force attack, its purpose is to defeat authentication mechanisms by trying to determine encryption-keys or passphrases by trying multiple likely possible combinations, such as words from a dictionary or a list with breached passwords.

Data breaches happen all the time, only in 2020 in the United States happened 1001 data breaches, that exposed 155,8 millions of records [7]. These breaches can include various personal details about customers, such as usernames, e-mail addresses, passwords (in cleartext or hashed form), IP addresses, etc. Then, the lists with these information can be found for sale in darknet or clearnet markets or even for free, and used to launch a dictionary attack.

The process of a dictionary attack is to utilize these lists of breached credentials to get access into accounts and password protected files. It is a common practice for users to use weak credentials as a way to remember them easily. It is worth to be mentioned that NordPass reports that the most used password (from the ones that were breached) was ”123456” [8].

The fact that a lot of users insist using weak passwords, along with password reuse in multiple occasions (accounts, wi-fi, root passwords, etc), makes dictionary attacks a prevalent threat, as for the easier, and most used, passwords it takes less than a second to crack them [8].

4. Conclusions

Miscellaneous challenges are a fun way to introduce CTF participants into subjects that are not traditionally related with the field of computer security, such as esoteric programming languages. About the subject of dictionary attacks, the best way to counter these type of attack is the extensive use of different passwords, or even better, random generated passwords and password managers.

References

[1] D. Temkin, Language without code: Intentionally unusable, uncomputable, or conceptual programming languages, Journal of Science and Technology of the Arts 9 (2017) 83. doi:10.7559/citarj.v9i3.432.

[2] Esolang, 2020, Esoteric programming language, URL: https://esolangs.org/wiki/Esoteric_programming_language.

[3] B. Easter, Fully human, fully machine: Rhetorics of digital disembodiment in programming, Rhetoric Review 39 (2020) 202–215. doi:10.1080/07350198.2020.1727096.

[4] B. Raiter, ,, Brainfuck an eight-instruction turing-complete programming language, URL: http://www.muppetlabs.com/ breadbox/bf/.

[5] Esolang, 2015, Pikalang, URL: https://esolangs.org/wiki/Pikalang.

[6] Blake Grotewold, 2018, Pikalang - the pikachu programming language, URL: https://github.com/groteworld/pikalang.

[7] J. Johnson, 2021, Cyber crime: number of breaches and records exposed 2005-2020, URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[8] NordPass, 2020, Top 200 most common passwords of the year 2020, URL: https://nordpass.com/most-common-passwords-list/.