THE UNIVERSITY OF HONG KONG

DEPARTMENT OF COMPUTER SCIENCE

A Platform for Cybersecurity Training and Holding Capture the Flag (CTF) competition

Supervised by Dr. S.M. Yiu

Group Members:

Han Yu (3035141736)

Yau Cheung Him (3035187572)

CHIU Kwan Yau (3035123241)

Catalog

1. Introduction

Nowadays cybersecurity issues are becoming more and more serious as information technology is infused into every part of our life. For all the electronic devices working with digital data, security vulnerabilities can easily lead them to malfunction and cause financial loss or even physical injury to users. Therefore, cybersecurity professionals are in a great demand in IT industry. It is predicted that about 3.5 million cybersecurity jobs will remain unfilled by 2021 (Cybersecurity Ventures, 2017). In order to efficiently select professionals and cultivate the interest of the young, many different events are held all over the world to draw people's attention to this area, main branch of which is Capture the Flag (CTF) competition.

Capture the Flag (CTF) is currently held in many countries by different organizations or even individuals to evaluate participants' skills in dealing with cybersecurity problems. It is also a good platform for users to apply theories to the real work and get hand on exercises. There are three traditional styles of CTF competition, jeopardy style, attack and defense style and a mixed style of the former two. In jeopardy style CTF, participants are required to solve problems provided and submit the solution to get the grade, while attack and defense pattern required participants to attack others' systems as well as maintain their own assigned service (Harmon, 2016). Moreover, for some large-scale CTF competitions, a mixed pattern of the above two styles are preferred. For example, DEFCON CTF uses jeopardy style in the first online round and adopts attack and defense style for the last round. There are many CTF open source platforms could support such competitions and this report will elaborate more about these platforms in the *Related Work* section.

Aimed at training students in this field, the University of Hong Kong (HKU) established the cybersecurity lab to provide training platform for simulating the CTF competition. Thus, a newly featured CTF platform is needed, which includes not only mixed style competition mode but also training mode with a large number of well selected training materials.

This CTF platform will employ the database containing questions and tasks of jeopardy style. And it will also manage multiple virtual machines to hold hacking and defense style competition for at least two teams. Furthermore, for short term training workshop, the platform will provide available training materials and keep track of the learning process for the students.

2. Related Work

Famed CTF competitions nowadays include DEF CON CTF, UCSB iCTF, Facebook CTF and PicoCTF, most of which are held with the help of open source CTF platforms. In this section, different available CTF platforms will be analyzed and compared with each other.

CTFd is a generalized open source platform which provides very basic functionalities for holding a CTF competition. One important feature of it is the generous allowance of customization which allows the users to add a wide variety of plugins to support their desired functionality. It automatically supports jeopardy style competition and provides challenge board for administrators to update. Adding plugins to hold attack and defense style CTF is also feasible, which, however, requires huge amount of effort.

Used by Facebook to hold CTF competition, FBctf only supports jeopardy style originally but can also be customized by modifying its source code. In contrast with python-developed CTFd, FBctf is constructed with a less common programming language Hack, a dialect of PHP developed by Facebook, which makes it more difficult to be customized (Chung, 2017) .

iCTF is a famous CTF platform that is aimed to support attack and defense style CTF competition and it is developed by University of California, Santa Barbara (UCSB). It assigns a virtual machine (VM) to each team and hides the flags inside it. Each team has to patch their own VM and exploit others' VMs for flags at the same time (The SecLab Group in UCSB, 2014). Other services including Central database and Scorebot take care of the communication between VMs, data storage and monitoring the status of flags. But one disadvantage of this platform is the long setup time since the preparation of VMs requires a lot of work.

Besides, there are also some platforms for cybersecurity training, including picoCTF and CyTrONE. picoCTF is designed to teach high school students with basic cybersecurity knowledge via video games (Chapman, Burket and Brumley, 2014). CyTrONE could setup training environment based on the user specification, such as firewall configuration, malware configuration and so on, and record the skill levels of the users. The CTF platform that is going to be developed in this project will try to create an enjoyable and relaxing training environment with the flexibility to monitor and adjust the learning pace of the user.

3. Objective

Last year, HKU established a cybersecurity laboratory to provide resources for students to learn and practice security skills. However, there is still a lack of software resources for training. Therefore, a software platform is needed to be installed in the computers in the laboratory and allow the students to learn by themselves or with suitable tutor.

3.1 Provide Training Resources

One main goal of this platform is to provide cybersecurity training for students. Students are expected to be familiar with real life security scenarios after using this platform. A wide range of tasks and problems will be provided for students to solve. They will be categorized by topics and difficulty levels, and some of the tasks are provided with self-learning materials. Students can access the platform any time and try the tasks with the aid of the materials in the platform.

3.2 Simulate CTF Competition

The platform will provide two training patterns: jeopardy style challenges, and attack and defend competition or training.

3.2.1 Jeopardy Style

For jeopardy style challenges, different categories will be included, such as Web, Forensic, Crypto, Binary, Reverse engineering and so on. Participants are required to find the answer (or called the "flag") of the question. As shown in table 1, these problems correspond to various security scenarios and cover a wide range of real life issues.

Web	The answer is hidden in a website and the attacker needs to find it with different methods
Forensic	The answer is hidden in a static data file and the attacker needs to analyze the data file to find the key
Crypto	The answer is encrypted with a specific rule and the attacker needs to decrypt it
Binary	The answer is stored in a compiled application and the attacker needs to exploit it with different methods to find the answer.
Reverse Engineering	The answer is in an executable file and the attacker needs to reverse the compiled executable file, and find the original input.

Table 1: Details about different categories of challenges to be covered for jeopardy style.

3.2.2 Attack and Defense Style

For attack and defense part, the platform will be able to host an event, where different virtual machines set up by the participants are connected to a host server through the platform. There may be some information or vulnerable services (or called the "flag") in each machine, and the goal of the participants is to get the information or services located in the others' machine and get score. The participants need to use their security knowledge to hack other machines, and also defend their machine from being hacked. This event allows different participants to interact with each other live time. During the whole process, the host server will monitor each virtual machine to count their scores and upload to score boards.

4. Methodology

The project could be divided into preparation part and implementation part. The preparation part will include three progresses - project planning, references collecting and question collection. After the preparation, the project will start the implementation part. In this part, the project will be implemented following the plan and the prepared material will be used to assist the implementation.
The detailed methodology is shown below:

4.1 Preparation

For developing Jeopardy style CTF, a database containing copious problems is needed. Some questions collected from internet will function as references in this process. After understanding and analyzing of these references, a new question set will be developed for this project.

4.2 Implementation

For the Jeopardy style, the implementation consists of two parts. Firstly, the developed question set will be stored into the database. Also, the platform, which will be developed with python, will be constructed to connect to database for user to retrieve questions. This platform will also adopt plugin which allows users to upload and check coding answer.

For the attack and defence part, the project implementation plan will be divided into two parts including admin part and user part. In admin part, it utilizes a central database to store the game state, a master program to host the scoreboard and monitor the status of the running VMs. In user part, it contains a user virtual machine with vulnerabilities. The open source tool security Scenario Generator (SecGen) has a modular architecture that can dynamically generate vulnerable security circumstances. It may be used to help provide such virtual machines in the competition.

5. Project Schedule

<table>
<tr><td>Timeline</td><td colspan="2">Task</td></tr>
<tr><td>1/9/2017 - 30/9/2017</td><td colspan="2">Analyze available CTF platforms and read relevant research papers</td></tr>
<tr><td>1/10/2017 - 15/10/2017</td><td colspan="2">Design the detailed framework for the platform</td></tr>
<tr><td>16/10/2017 - 10/11/2017</td><td>Construct the part of platform that supports jeopardy style challenges.</td><td>develop the problem set involved in the jeopardy style</td></tr>
<tr><td>11/11/2017 - 20/12/2017</td><td rowspan="2">Construct the part of platform that supports attack and defense style challenges</td><td>customize the SecGen to help generate VMs according to specifications</td></tr>
<tr><td>21/12/2017 - 10/1/2018</td><td>develop multiple versions of VMs with different security vulnerabilities</td></tr>
<tr><td rowspan="2">11/1/2018 - 22/1/2018</td><td colspan="2">First Presentation</td></tr>
<tr><td colspan="2">Intermediate report</td></tr>
<tr><td rowspan="2">23/1/2018 - 1/3/2018</td><td colspan="2">Construct training system of the platform.</td></tr>
<tr><td colspan="2">Develop both online and offline training materials</td></tr>
<tr><td>2/3/2018 - 10/4/2018</td><td colspan="2">Testing the platform</td></tr>
<tr><td>11/4/2018 - 20/4/2018</td><td colspan="2">Final Report and Final Presentation</td></tr>
</table>

6. Reference

Cybersecurity Research and Market Intelligence, (2017), Cybersecurity Ventures. Retrieved from:https://cybersecurityventures.com/jobs/

Harmon T, (2016, 14 September), Cyber Security Capture the Flag: What is is? Cisco Blogs. Retrieved from: https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it

Chung K, CTFd LCC, (2017), The Advanced Computer System Association (usenix). Retrieved from: https://www.usenix.org/system/files/conference/ase17/ase17_paper_chung.pdf

Vigna G, Borgolte K, Corbetta J, Doupe A, Fratantonio Y, Invernizzi L, Kirat D and Schoshitaishvili Y, The SecLab Group, University of California in Santa Barbara, (2014), The Years of iCTF: The Good, The Bad, and The Ugly, The Advanced Computer System Association (usenix), Retrieved from: https://www.usenix.org/conference/3gse14/summit-program/presentation/vigna

Chapman P, Burket J and Brumley D, (2014), PicoCTF: A Game-Based Computer Security Competition for High School Students, The Advanced Computer System Association (usenix), Retrieved from: https://www.usenix.org/system/files/conference/3gse14/3gse14-chapman.pdf

Z. Schreuders C, Shaw T, Shan-A-Khuda M, Ravichandran G, Keighley J, Ordean M, (2017), Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting {CTF} Events. Retrieved from: https://www.usenix.org/conference/ase17/workshop-program/presentation/schreuders