Jurnal Integrasi
Vol. 14 No. 1, April 2022, 14-22
e-ISSN: 2548-9828

Article History
Received January 2022
Accepted April 2022

Analysis of Cyber Security Knowledge and Skills for Capture the Flag Competition

Jean Tirstan T[*], Joy Gilbert A[*] and Nelmiawati[#]

Politeknik Negeri Batam
*Cyber Security Engineering Study Program
[#]Informatics Engineering Department
Jln. Ahmad Yani, Batam Centre, Batam 29461, Indonesia
E-mail: jeant2212@gmail.com, joygilberta@gmail.com, mia@polibatam.ac.id

Abstrak

Kompetisi CTF (Capture the Flag) telah muncul sebagai instrumen penting untuk pengembangan pendidikan keamanan siber dalam enam tahun terakhir. Sangat penting untuk memastikan bahwa kompetisi CTF terus berkembang mendukung pertumbuhan pendidikan dibidang keamanan siber. Untuk mencapai pertumbuhan yang diinginkan, perlu dilakukan analisis untuk kemajuan yang telah dicapai dalam enam tahun terakhir program telah dilaksanakan. Penelitian ini mengumpulkan dan menganalisis kurang lebih 500 solusi CTF dari platform CTFtime. Dari hasil analisis tersebut, kami telah mengidentifikasi bahwa dibutuhkan kemampuan dan teknik pada setiap masing-masing kategori soal CTF. Hasil analisis ini kami gunakan sebagai acuan soal pada Platform CTF yang kami buat saat kaderisasi PCT (Polibatam Cyber Team). PCT terdiri atas sekelompok mahasiswa program studi Rekayasa Keamanan Siber yang dipersiapkan sebagai garda terdepan dalam mengikuti berbagai kegiatan yang berkaitan dengan perlindungan Keamanan Siber. Metode yang kami gunakan berbeda dengan CTF lainnya, dimana kami menggunakan pendekatan berbasis kemampuan dan teknik. Kami menemukan bahwa metode pendekatan ini mampu menarik 80% peserta dalam memecahkan dan meningkatkan kemampuan mereka dibidang Keamanan Siber terhadap setiap tantangan dalam lingkungan yang kompetitif.

Kata kunci: CTF, CTFtime, Keamanan Siber

Abstract

CTF (Capture The Flag) competitions have emerged as a pivotal instrument in development of cyber security education over the past six years. It is imperative to ensure that the CTF competitions continue to develop to facilitate growth of cyber security education. To achieve the desired growth, it is necessary to analyze the progress achieved in the last six years the program has been implemented. This research collects and analyzes approximately 500 CTF solutions from the CTFtime platform. From the results of this analysis, we have identified that skills and techniques are needed in each category of CTF questions. We use the results of this analysis as a reference for questions on the CTF Platform that we created during PCT (Polibatam Cyber Team) regeneration. PCT consists of a group of students from the Cyber Security Engineering study program who are prepared to be at the forefront in participating in various activities related to Cyber Security. The method we use is different from other CTFs, in that we use a skill-based and technique-based approach. We found that this approach was able to attract 80% of participants in solving and improving their skills in Cyber Security towards any challenges in a competitive environment.

Keywords: CTF, CTFtime, Cyber Security

1. Introduction

Introduction of academic Capture the Flag competitions revolutionized the study of cyber security significantly. The academic competitions have attracted many participants, including students and professionals who aim at improving their cyber security skills. The introduction of the competition was conceptualized as an attempt to address the expanded desire of a large group of cyber security enthusiasts to participate in the competitive challenges. Therefore, the program was incorporated to extend the educational objective of the competitions to many people. Since it was introduced, there have been multiple competitions organized for this category which have had significant results in terms of the growth of the learners in the cyber security space. The influence of implementation of the program has been felt across different schools across the world. Consequently, the existence of the academic competition has been popularized, resulting in an increase in the number of participants who register to compete for in the challenges. The past six

years have seen a significant increase in the sign-ups of new competitors seeking security education.

In this research study, we collected data from writeups and from different academic competitions organized in the past six years. In this period. Much effort has been invested in the development of a conducive environment for this category of competitors to grow their skills. At the onset, several students who signed up for competitions complained of the complexity of the competing platform, making most of them lose hope. However, since this observation was noted and worked on, the system has been greatly handy for most users who are not proficient with cyber security concepts. The competition platform provides suggestions to the users whenever they are stuck in a particular step. Although the system provides them with a way out of difficult situations, the learners are not fed with the solutions to their challenges. Instead, a thinking pattern is provided that helps them think in a particular line of thought that leads them to the solution to the impending challenge.

An assessment of the effectiveness of different strategies is dependent on the ability of these strategies to effect change on the involvement of the newbies in the competitions. Singular analysis of the impact that individual mechanism has had on the overall population of the participants who participate in the competitions and their corresponding performance in the competitions is done. This study will take into account the reports indicated by the participants who seek to join the cyber security by undertaking an evaluation of the feedback and reports they provide upon participation. Implementation of these recommendations will be handy in designing a definitive improvement mechanism for enhancing the development of cyber security experts.

There are distinct gaps and discrepancies between the demand for good quality admissions procedures and the lack of methods to do this. Then we can see activity cyber security assessments in academies cannot only be seen and judged based on traditional knowledge [1]. As a general rule, task arrangements are fundamentally founded on the methods that should be applied and the instruments for playing out those strategies. Nonetheless, applying strategies and utilizing devices requires information and abilities to help the activity [2].

The data analyzed reveals that most competitions undertaken in the past six years by the academic category are majorly jeopardy tasks. Thus, it is imperative to infer that the students have developed analytic skills. Therefore, the new development design will focus on an attempt to develop other skills that make the students all-around security practitioners. Some of the recommendations that will be made include the suggestion of a plan to incorporate a collaborative mechanism for growing the skills [3]. An improvement should also be made on the operational flow of the website to facilitate ease of navigation.

Information used in this evaluation was obtained from GitHub repositories where participants have posted their writeups. Writeups in GitHub are organized in a sequential manner allowing for easy retrieval. The writeups contain the participant's accounts of the experience they had undertaking the competition. Through the writeups, we derived the issues that the students found challenging. They also contain the specific point of weakness that the students are not competent in. From the analysis, we establish a pattern of the challenges that the students face undertaking the competitions and their strengths. A relative graph was established relating the interventions and the success rate from the impact on the competitors. Another material used in the study is the CTFtime.org website. The website helped trace the number of participants who participated in individual events hence creating a logical pattern.

Therefore, this work will be structured in sections that address different topical evaluations. First, the related works section will investigate similar work done previously relating to the development of cyber security education through the use of the CTF competitions. This literature review will cover articles written exclusively within the CTF organization. The subsequent section will discuss different steps undertaken to ensure the growth of security education. This section examines different interventions put in place to ensure the growth of the field. The progress of different interventions such as the exercises, set up for the new participants and success of the mechanisms by discussing the results of using the platform and performance in the exercises introductory computer course.

2. Related Works

The development of security education has been the epicentre of most of the technological interventions made by different stakeholders to nurture more talent in the cyber security space. The interventions have involved the development of tools and programs aimed at equipping the learners with the necessary skills to guarantee their excellence in the discharge of the mandate of cyber security. Different incubation centres have been developed outside schools and within schools with the aim of encouraging more participants to join the ever-growing technological group. The success of these interventions has been a significant increase in the number of participants who enroll in different competitions to exploit their skills by evaluating their expertise against those of other people with similar skill sets [3]. Different developmental strategies put in place have yielded fulfilling results. On the contrary, a good number also does not achieve the targets they set to meet. As a result, some have dwindled and died away in the wake of competition from other revolutionary strategies such as the CTF

competitions. Interventions that have stood the test of time have been those that have bestowed the responsibility of motivation and sustaining the dream with the learners themselves. Those who have centralized the dream of achieving a larger number of new recruits have failed to share their dreams and aspiration with the candidate they train, making them die away faster.

Therefore, several documentations have been made with regards to these interventions aimed at growing the population of the security participants. Notably, the CTF competitions have been outstanding in this venture, given the dynamic strategies employed to meet this target [1]. Particularly, gamification and massive recruitments of participants in colleges have been successful since the student's desire to associate with an environment that challenges them to become better versions of themselves [4]. Many CTF competitions have been presented as online games attracting more users given the presentation of the ideas are appealing. Moreover, online engagement has become the norm due to its flexibility in terms of time and time allocation. Additionally, the online hosting of the competitions allows for the desired anonymity in the cyber security world.

Different online CTF competitions hosted in varied platforms show a difference in performance due to the varied features of the different platforms. The diversity of the features causes a corresponding difference in the efficiency of the platforms resulting in a biased outcome. Automation has been incorporated in many platforms to encourage the unsupervised management of the platforms and adjustment of the features based on the needs of the user. As a result, the platforms have become efficient and faster. For instance, automatic flagging was enabled to ensure that new users were accustomed to the functionality of the platforms enabling them to develop skills that allow them to navigate through tougher and more complicated platforms. PicoCTF [5] is an example of a platform that is downloadable and can run offline, enabling the users to undertake more practice with the exercise before engaging in actual online competition. This feature has helped many new users to help understand the platform well before engaging in actual competitions.

An evaluation for a previous study reported that the design of the content presented to the beginners was too difficult for them to handle hence not serving their educational needs. Therefore, a revision was made to ensure that the information presented to the beginners suited their level. A revision of the outline of the content they were introduced to was conducted, and the results significantly improved. The implication of this intervention is the increase in the number of newbies who go beyond the introduction stage and become incubated into the field successfully. Educators are seen in different contexts to be responsible for the success rates of the integration of new students into the field since their understanding of the educational needs of the new learners determines whether the students will transition from being newbies to becoming techies.

3. The Material and Research Methodology

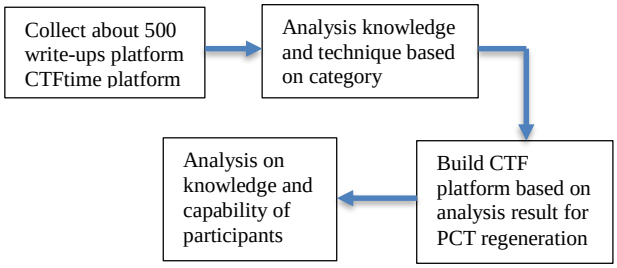

Figure 1. Research Methodology

Figure 1. shows research methodology that we used in this study. We collected 500 CTF solutions from various competitions. From the results of this study, we analyzed the techniques used based on each challenge category. Subsequently, we setup a platform to analyze the capabilities of PCT cadre participants as a form of implementation of the analysis we got.

3.1 Platform Setup

Platforms in which the competition is hosted significantly influence the performance of different players. This is particularly a great deal for beginners since the problem can have far-reaching implications for the performance of the competition if they do not configure the platform correctly. Setting up platforms has been a big challenge to many beginners who seek to participate in the CTF competitions [4]. Although this can be viewed as a trivial issue to the competitors who have mastered the competition, the challenge is huge and implicative for new users who are not adequately conversant with how the platform works and how to navigate through.

As a result, PicoCTF was released to allow beginners to practice before they can engage in actual competition. The platform is downloadable and operates offline. The provisions of the platform allow the users to experience the actual feel of a real CTF competition, making the platform a revolutionary instrument in developing the experience necessary for the students to participate in the competitions. It is retrogressive to incapacitate a user from participating in the competition because of the inability to set up the platform. Despite not contributing any points in the competition, the platform setup has extensive implications for the performance of a user.

Setting up the platform has been streamlined in different distributions of the existing platforms. Platforms available for use that adequately prepares the students for participation in the CTF competitions include PicoCTF [5], OpenCTF [6], CTFd [7], FbCTF [2] and TinyCTF [8]. Installation of two of these platforms is vagrant, while other two are native. OpenCTF requires docker installation to set up.

Setting up these platforms requires a high level of expertise which may not be the case with the students who have just joined the field. Consequently, the interventions made to release the downloadable platform have realized an increase in the number of students who have grown their capacity to sufficiently set up a platform for the competition. The implication of this intervention is that more students are capable of participating in the competitions allowing the growth of security education [9].

Understanding and exploiting platform features such as user management, problem setup, web interfaces, grading problems, players statistics, and team management is vital in the optimization of the outcomes of a participant in a competition. A deep understanding of the benefits of these features and the capacity to leverage them for operational advantage places the competitors in a higher position to become competent and productive in the field. Thus, it is imperative to recognize the influence that the use of the offline platform has had on the overall success of the learning of the students.

To evaluate the educational value derived from the implementation of the offline setup platform, we investigated the performance of the competitors under the academic tier to determine the performance of those candidates who began with installing the downloadable PicoCTF platform [5]. The assumption that their success or failure is determined by the efficiency of the platform in preparing the candidates in real competitions was made. Thus, the findings of the investigation indicated that students who practiced with the offline platform before enrolling for the competitions performed better than those who opted to sign up for the competition without prior preparation. The results indicate that the failure of the competitors was not caused by a lack of adequate security skills. Instead, challenges setting up the platform derailed their morale significantly, making them lose hope in the competition. On the other hand, those students who used the PicoCTF before the main competition was more confident and could navigate faster and efficiently. Therefore, it is imperative to recognize the influence that the complexity of installation has on the development of education of security learners.

Several learners have registered sluggish growth at the onset due to the lack of proficiency in the installation and setup of the platform where the competition occurs. Many users who had an interest in learning the field failed to pursue the field for the same reason. Demanding the students to understand how to configure a platform using python or PHP at the onset is demanding too much from a naive but enthusiastic learner. Therefore, the development of cyber security education is influenced by the complexity of undertaking complementary setups such as installation since it contributes to the overall ability to undertake the CTF competition efficiently.

3.2 Exercises

Exercises are instrumental tools designed to improve the competency of the students in cyber security. The tool was instituted to prepare the students for actual competitions and impending challenges and tasks [10]. The students are provided with challenges identical to those they will face in actual practice to allow them to develop the skills required to complete the task. Determination of the student to successfully solve the problem demonstrates the students' commitment to tackle real-world security challenges. Therefore, the exercises are categorized into different groups based on the skill that the educators seek to develop in the learners. An analysis of the frequency of the exercise topics emphasizes the prevalence of such problems in the environment. Thus, the designers of the exercises aimed at developing the most prevalent skills in students since they would be challenged with such problems more often.

Previous analytic studies reveal that some categories of security problems are more prevalent than others. An investigation conducted previously on CTF competitions done between 2011 and 2016 reveal that categories named ‘crypto’ were the most prevalent among the over 160 challenges investigated. ‘web’ challenges had a competing number of occurrences. ‘reverse’, ‘forensic’, ‘pwn’, ‘misc’, ‘exploit’, ‘stegano’ and ‘ppc’ followed respectively. These categories exemplify the prevalence of such challenges in the market, hence qualifying the need to develop skills in these categories.

Therefore, the developers of the exercises scheduled them such that the most prevalent category was put more emphasis by increasing the frequency of their occurrence. This explains why crypto exercises were more prevalent in the exercises than other types of exercises. Consequently, the students develop the most common skills at the onset, preparing them for bigger challenges that are not more prevalent. The existence of 77 unique categories of the exercises implies that there are diverse groups of security challenges that a beginner can practice at any given time. Educators highly advise the learning approach that focuses on the simple concepts at the onset of the studies, followed by progressive advancement towards the complex concepts [9]. Notably, the more common challenges are evidently easier to undertake than those that are rare. This is statistically true due to the fact that their high frequency has necessitated extensive research and exploitation. As a result, several learning materials become available for any student seeking to learn the concepts. The opposite is true for rare challenges; the rarer challenges attract less scrutiny and research due to their lowered frequency. Consequently, anyone desiring to venture into the topic will do more hands-on research to obtain some fundamental concepts due to unavailability. Therefore, the more frequent

exercise categories are easier to learn because more learning materials are available to the same effect, unlike the exercise categories with lower prevalence.

3.3 Exercise Difficulties levels

CTF competitions have a different range of sophistication. The complexity determines how much effort is required to complete the task. In the development of security education, it is imperative to recognize one's capability by knowing which difficulty level one can solve. The difficulty levels are categorized into three distinct groups based on the technical requirement demanded by the task to complete. This categorization of the levels is essential in tracking the skills growth of a beginner in the cyber security space.

The three levels are; easy, medium and hard. Easy category contains those challenges that require one or two tricks and a single tool to solve. The easy challenges can be tackled by beginners. All they would need to solve the challenge is to follow the writeup keenly and implement the steps provided. The writeups of such challenges are easy to understand since they contain a direct description of the steps that one would require to complete the task [10]. This level is useful in the development of the skills of beginners. They help bolster the confidence of the beginners by demonstrating that accuracy yields output. Solving these challenges at the beginning validates the concepts presented in subsequent events since it helps the learners that adherence to procedure and the rules yields results rather than the random organization of concepts. Previous results indicate that the 'msc' category has more easy challenges than any other category in cyber security since they are used to test general programming and mathematics principles. Exercises of this difficulty level have extensive implications on the development of learning in security since it instills the appreciation of logic and procedure.

On the other hand, medium-level exercises require three or more tricks and tools to solve the challenge. Reading the writeups alone is not enough for a beginner to solve the challenge. They require to undertake more analytical studies to obtain more skills to support their knowledge. One or two extra resources are handy to enrich the beginners with the required principles and technical capacity to complete the challenge. Students who can solve this must have had an in-depth conceptualization of the basic principles of cyber security. Hence, obtaining more information builds on an existing knowledge base. This level of difficulty is essential in challenging the learners who are capable of completing easy challenges to improve their skills by taking on more sophisticated challenges [11]. The medium level prompts the learners to continue engaging in continuous learning. Challenges in this difficulty level demand a beginner to put more effort into acquiring more knowledge about different principles and their applications.

Challenges in the hard difficulty level require a deep understanding of the concepts of cyber security to complete. Several legendary tricks and tools are consolidated to solve challenges at this level. A beginner can hardly understand the contents of the writeups at this level, let alone implement them. Learners require progressive mastery of concepts in order to integrate the different tricks to solve these problems. Thus, a learner who can solve medium level challenges would require to undertake extensive research to complete these tasks [12]. They would take a long to solve the problem due to the need to gather the knowledge required before thinking of an effective mechanism to solve the problem.

The existence of a definitive category of difficulty levels allows the students of cyber security to grow gradually through the levels. Previously, before the difficulty levels were distinctly cut out, many starters would get frustrated by their inability to complete a problem because they would be exposed to challenges of different difficulties. Thus, it is worth noting that the implications of the definite distinction of the difficulty levels have influenced significant development in security education. The students can now take progressive learning recognizing their level and capabilities. This helps bolster the confidence of the beginners in the process hence enhancing discipline's growth.

3.4 Skills

Cyber security demands proficiency in different skill sets to undertake cyber security functions efficiently. The development of these skills demonstrates competency in the field. Therefore, the ability of the learners in a system to develop these skills determines the efficiency of the learning system to nurture cyber security skills. Thus, in evaluating the development of an institution's cyber security development level, it is essential to evaluate how well the students grow these skills. The skills act as indicators of the existence of a robust learning system where students can thrive to become competent cyber professionals. These skills include; coding, cryptography, reverse, pwn, forensic, and web [9]. They are the main categories of the exercises organized in the CTF competitions. Thus, this study seeks to evaluate how efficiently they have been developed among the students by assessing the performance of the participants in the CTF competitions of this nature.

3.5 Coding

Coding is a fundamental skill in cyber security. The skill is the medium of communication that allows participants to interact with the computer systems by writing commands and receiving responses that indicate certain changes. The skills are a basic tool in the implementation of different thought processes

programmatically. Cyber security practitioners require a good understanding of coding to establish the flaws in the association of different elements of a system. Participants require coding skills to undertake data processing [13]. Coding is also used to send and receive packets of data from servers. Mastery of these coding skills demonstrates a person's ability to undertake data-related processing.

Fundamental coding skills expected of a participant include the ability to convert numbers and letters from one format to another. This is a crucial skill since elements in computer languages are represented in different formats other than the human-comprehensible values such as variables and characters. Mastery of ASCII characters, hexadecimal numbers and Base64 strings is fundamental in practice as a security expert. Demonstration of progress in the understanding of these skills points to an efficient learning system.

Moreover, the learners must grasp programming languages that are significant in the execution of their duties. Python has been outstanding in the cyber security scope since it provides a dynamic and interactive way of communicating with the systems. Python is easy to learn and use compared to other languages such as the assembly language. Thus, the participants should master this coding aspect since it is the communication medium for all participants who seek to venture into cyber security.

Network programming is also an important aspect of coding that a cyber security practitioner cannot fail to have. Since it is a common experience to link different devices through different ports, it is imperative that the participants learn these fundamental concepts and become equipped with the technical know-how of manipulating different networking concepts. One's significant application of this concept is in setting up the platform where the CTF competitions are hosted. The participants are expected to establish a connection through which they can share packets of data.

Thus, the establishment of a robust system that is aware of the coding needs and seeks to nurture these skills implies that it is an efficient system. CTF competitions have been designed to test these skills extensively. The entire communication mechanism is presented as code. The participants are expected to learn to interpret these concepts accurately in order to participate in the competition. Coding is treated as the bare minimum requirement for any participant to take part in the competitions. The CTF competitors have all demonstrated a mastery of the coding skills through their use and understanding of the coded language. Developers of the competition designed the competitions such that it encourages extensive understanding of the codes. This intervention seeks to bolster the development of the participants in coding.

3.6 Cryptography

Challenges in the 'crypto' category involve the analysis and establishment of cryptographic flaws in different systems. The cryptographs seek to exploit vulnerabilities in systems in order to attack. Therefore, cyber security practitioners should be able to understand a majority of the existing cryptographic algorithms that are commonly used. Familiarity with the structure of the algorithms is not sufficient to become a cyber security expert. Instead, the participants will also need to be able to understand how the algorithms attack the systems.

Common cryptographic algorithms that are well known to most cyber security practitioners are the RSA algorithms. Moreover, hash algorithms are the second most popular cryptographic algorithms registered in cyber security. Other groups of cryptographic algorithms that are common include the custom group, which contributes 37.3% of the problems recorded in cyber-attacks. The most common custom cipher is the XOR. The symmetric group has the largest number of ciphers that include AES and Caesar, and contributes 34.4% of the problems recorded. The asymmetric group is the third largest group with ten ciphers that include RSA and ECC. They are most commonly used. Hash algorithms include MD5 and SHA1/2, and they contribute 5.3% of total problems in the cyber security space. Misc group has four known ciphers, including DSA and SSL. These algorithms are the most commonly encountered algorithms. This statistic is supported by the frequency in which they have appeared in the CTF competitions. The high or low frequency of the occurrence of any particular cryptographic algorithm in the competitions reflects their prevalence in the actual field.

The developers of the competitions ensure that they represent the actual environment of the cyber security space. The structure of the crypto exercises that emerge in the competitions demonstrates the prevalence of crypto in the market. The existence of a robust and dynamic system to frequently align the contents of the competition with the environmental experience reflects the effort that the educators put into ensuring that the learners who emerge are obtaining the right skills that prepare them for the awaiting market. Thus, the learner needs to grasp the contents of the competition to remain relevant in the dynamic environment. The flexibility of the CTF competitions allows it to streamline its competitions with regard to the prevailing market needs.

3.7 Forensic

Forensics is the process of extracting malicious information hidden in other harmless objects. This skill is essential to participants who seek to engage in cyber security since they will always need to be careful not to allow vulnerability by exposing themselves to danger, and also, they should be able to embed their code or items in other objects to bypass

some physical security checks such as the human eye. Different skills are essential here, including that of embedding hidden flags in images. The participants learn these skills early into the cyber security profession in CTF. As a result, they become proficient in the needs they are supposed to meet.

An evaluation of the CTF competitions reveals that the learners who have grown professionally in the competition are equipped with the necessary skills to undertake these tasks. Network trace challenges are also a crucial practice in forensics since it is the channel through which attackers use to attack the system. PCAP files are presented with hidden flags allowing transmission without detection. However, cyber security practitioners must be able to flag this suspicious activity.

Another common occurrence is the use of multimedia files to present hidden flags. The attackers use audio and video files to hide and transmit malicious flags intended to cause harm to the recipient. The participants should have a deep understanding of data types to distinguish the malicious files and flag them. Therefore, an extensive research study is undertaken to acquire this knowledge. The frequency of the occurrence of forensic competitions in CTF illustrates how the educators in the platform are dedicated to ensuring the development of this fundamental skill.

3.8 Web

Web challenges require an extensive understanding of web technologies. The technologies are presented on both the client and the server-side. The server side requires security experts to be conversant with the building frameworks that are used to develop the servers. The technologies include PHP language, SQL language and MySQL database. The technologies make up the parts of the server-side of the web technology. On the other hand, the client-side requires that cyber security practitioners develop their JavaScript and HTML skills to understand how the HTML tags contribute to the overall structure of the web pages.

The most common web attack is SQL injection. Since websites are made up of interconnected databases and web pages, where the webpages sources data from the database to provide dynamic interaction with the client, attackers exploit this connection to the database by instituting injections into the database in an attempt to retrieve restricted data. This type of attack is very common given the existence of SQL databases for a long period in the market. Moreover, HTTP exploits are also equally common due to the flaws that exist with the transmission of information through the HTTP configurations that may allow for vulnerabilities when it is not correctly configured. PHP suffered cross-site exploits due to its long use, which have made it to be more vulnerable than newly emerging technologies.

GIT has been exploited for vulnerabilities due to the fact that developers use its version control. GitHub became a target by attackers since they have been used to store software code that contains important information. In spite of the serialization and deserialization of objects on the web, it is not sufficient to make the web content secure and free of flaws. The vulnerabilities will continue to be exploited. However, the inclusion of the web challenges in the competition allows the competitors to write informative writeups that help improve the learning of other users who join cyber security later. This transfer of information from one user to another allows for the development of education about the cyber security of the web. These writeups become the basis for other studies since it helps expose the vulnerabilities that exist on the web. Thus, CTF competitions become exemplary incubation centers for new concepts and the revelation of new discoveries. The process allows for the growth of the research on different topics.

3.9 Reverse

Reverse challenges involve the flagging of embedded programs and exposing their presence. Players use assembly language to distinguish the executable code in files from the flags by thorough analysis. This process involves extensive analysis of the code to determine which code lines are flags. In the evaluation of previous reverse competitions, it was noticeable that most of the reverse competitions involved reverse engineering executable binaries running in Linux or Unix computers. Development of the skills and the technical capacity to solve this challenge requires extensive and specialized studies. The process is tedious, hence making it a rare challenge to occur.

However, CTF competitions ensure that the people who participate in their competitions are equipped with diverse skill sets. The designers of the competitions usually prefer to reserve the reverse challenges for the competitors with advanced skills. Therefore, the defined outline for the implementation of the academic competitions in the CTF competitions has significantly grown the educational base of the students. Continuous research and studies on this topic allow it to grow.

3.10 Pwn

Pwn challenges adopt a similar solution strategy as that of the reverse challenges since they involve the flagging of malicious embedding of malicious flags in commonly explorable items such as images, network, audio, disk, text, pdf, video and archive. Thus, just like reverse challenges, X64 and X86 assembly languages are also used to provide solutions in this context. Therefore, mastery of these concepts is handy in both pwn challenges and reverse challenges. Exercises of these categories are posted regularly based on three main flaws; format string, data

overflow, and function pointer overwriting. Learners are then able to use the competitions as a platform to gauge their capabilities against the learning objectives.

4. Lessons Learned and Observation

The study sought to determine if an efficient academic system had been established in the competitions of CTF. Therefore, we investigated the academic development of the students who were undertaking the academic CTF competitions. We identified random groups from random competitions from different competitions and administered a survey where we sought to determine their level of academic growth in cyber security. Moreover, the investigation sought to determine why it was significant for the students to engage in the competitions and what influence it had on their careers or life. Six random groups were selected, and the data was collected. The students' anonymity was guaranteed.

Moreover, we leveraged the CTFtime.org website to obtain the performance of the participants who took the interview. We collected their points and the writeups they produced for the competitions they participated in Figure 2.

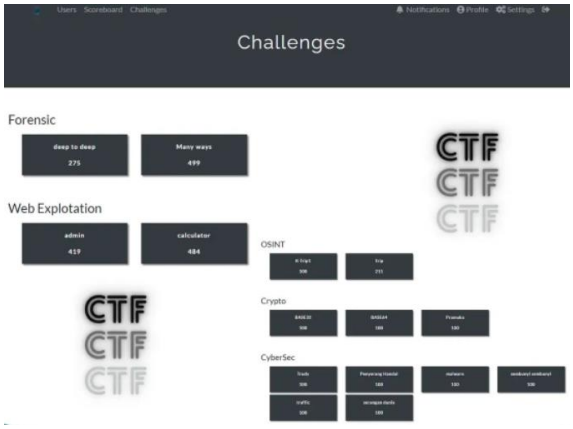

Figure 2. CTF-PCT Platform

The investigation revealed that most participants in the competitions were university students undertaking technology courses. Whereas others were actual students of cyber security, most of the surveyed population were passionate students who sought to explore new ventures in technology. The results of the survey on the regeneration of the Polibatam Cyber Team a definite learning pattern that involved going to class or self-learning from home. The students registered that the competitions academic CTF competitions provided a distinct and clear path through which one can grow. The students noted that the academic CTF competition competitions provide a distinct and clear path in which one can grow.

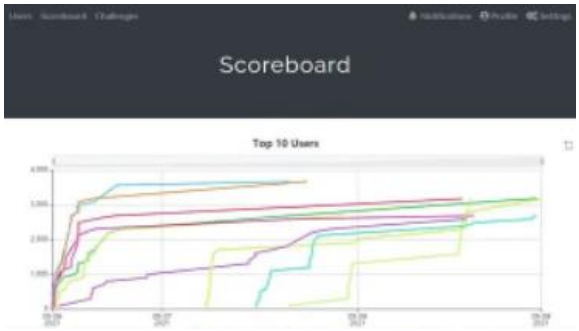

Figure 3. CTF Platform Scoreboard

Figure 3. shows an evaluation of their performance in the competitions. It shows that they are average performance who strive to become better. The writeups that one of the groups produced for a web challenge demonstrated mastery of concepts. The results showed consistent growth from previous writeups. The writeups demonstrated an average understanding of the fundamental cyber security skills.

4.1 Development of skills

Many cadre participants from PCT have a definitive skill development plan which is allowing them to grow their skills while participating in the competition. The students demonstrated the development of competency of basic learning objectives. Many students who enrolled have become proficient in coding. This has been demonstrated in the ability of all the participants who enroll for the competition to understand coding fundamentals that allow them to interact with the system efficiently.

Moreover, the development of the educative aspect of the competition is participants who compete in the academic CTF category have posted excellent results that show a progressive grow evidenced by the success rates of the beginners. The path in the knowledge they acquire. More participants had gradually increased since 2016, when the education program was conceived. Additionally, there has been an increase in the frequency of the competitions, encouraging the growth of security education.

4.2 Difficulty of exercises

Since the introduction of the education program, there has been progressive development of the students with the capability of tracking their career development. The categorization of challenges based on the difficulty levels has been instrumental in building a structured mechanism for tracing the growth of a learner. With the presence of these levels, it is easy to know which skills a learner has acquired based on the difficulty of the challenges they can complete. Many learners now know the level of proficiency they are in and are working towards moving to the next step.

The majority of the students who joined the competition started as beginners and then grew in skill to become more proficient, transitioning to

subsequent levels. There were 40 of 50 students who participated could achieve improvement within one month. 80% of those participants noted an increase in academic progress since the introduction of the academic competition. Through the introduction of the difficulty levels, the students engage in competition based on their abilities making the outcome more progressive in terms of growth of skill. The frustrations that would arise from beginners engaging in competitions beyond their level have been eliminated, and progressive competitions embraced. Therefore, it is imperative to recognize the influence that the establishment of a distinction between the three difficulty levels has had on the development of security education.

5. Conclusion

In this paper, we investigated the development of education in cyber security. The investigation involved the analysis of the educational progress of beginners who enrolled joined the CTF competition in the academic category exclusively. Upon conducting a thorough evaluation of the performance of the students, we registered that education in cyber security has significantly grown. The growth has been contributed by deliberate interventions put in place by the educators in CTF in an attempt to grow the cyber security scope. Specific measures put in place by the designers of the organization were effective in achieving the educational milestones realized today. Therefore, stakeholders must be recognized for their efforts to bolster the growth of the profession. A significant intervention that stood out in this quest for a definitive educational framework is the use of competition to effect change. The education level CTF competition has been instrumental in driving the change that has been realized in the cyber security space and the impact that will be felt in the future. The interventions made to achieve the current success will be viewed in the future as the foundation of conceptualization of competition for learning. From 50 students who participated, there were about 40 students who could achieve improvement within one month on the CTF-PCT platform that we created. 80% of those participants noted an increase in academic progress since the introduction of the academic competition.

Reference

[1] M. K., S. S., E. M. and M. O., "Using Technical Cybersecurity Exercises in University Admissions and Skill Evaluation," *IFAC-PapersOnLine*, 2019.

[2] H. A., R. H., I. A., Z. M. and R. F., "A CTF-Based Approach in Cyber Security Education for Secondary School Students," *Journal of Computer Science and Information Technology*, 2021.

[3] B. N., L. F. G., H. B., R. P., M. L. and L. L., "Cyber teaming and role specialization in a cyber security defense competition.," *Frontiers in Psychology*, 2018.

[4] A. Yasin, L. Liu, R. Fatima and W. Jianmin, "Improving Software Security Awareness using A Serious Game," *The Institution of Engineering and Technology*, vol. 13, no. 2, pp. 159 - 169, 2019.

[5] P. Matias, P. Barbosa, T. C. Cardoso, D. M. Campos and D. F. Aranha, "NIZKCTF: A Noninteractive Zero-Knowledge Capture-the-Flag Platform," *IEEE Security & Privacy* , vol. 16, no. 6, pp. 42 - 51, 2018.

[6] T. Burns, S. Rios, T. Jordan, Q. Gu and T. Underwood, "Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education," *ASE*, 2017.

[7] CTF Time, "CTF Time," [Online]. Available: https://ctftime.org/.

[8] S. Karagiannis, E. Maragkos-Belmpas and E. Magkos, "An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools," in *13th IFIP WG 11.8 World Conference, WISE 13*, Slovenia, 2020.

[9] F. Sharevski, A. Trowbridge and J. Westbrook, "Novel Approach for Cybersecurity Workforce Development: A Course in Secure Design," in *IEEE Integrated STEM Education Conference (ISEC)*, 2018.

[10] N. Elliot, D. Kendall and M. Brockway, "A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills," *IEEE Access*, 2018.

[11] B. Caulkins, T. Marlowe and A. Reardon, "Cybersecurity Skills to Address Today's Threats," in *In International Conference on Applied Human Factors and Ergonomics*, 2018.

[12] L. Khoo, Education Framework using Capture the Flag (CTF), Malaysia: IGI Global, 2019.

[13] M. Yamin and B. Katt, "Inefficiencies in Cyber-Security Exercises Life-Cycle: A Position Paper," in *AAAI Fall Symposium*, 2018.