A Scenario CTF-Based Approach in Cybersecurity Education for Secondary School Students

Ahmad Haziq Ashrofie Hanafi[a], Haikal Rokman[a], Ahmad Dahaqin Ibrahim[a], Zul-Azri Ibrahim*[a,c], Md Nabil Ahmad Zawawi[a,c], Fiza Abdul Rahim[b,c]

[a]*College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia*
[b]*Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
[c]*Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Malaysia*
*Corresponding author: zulazri@uniten.edu.my

***Abstract* – Cybersecurity education topics require technical understanding. However, it is a challenging task for any teacher to introduce topics to students who have no technical background. Recently, the concept of gamification has been implemented as a tool to inculcate student's interest using a variety of popular in-games techniques and to apply them to educational modules. Extending from this notion, it was found that the Capture the Flag (CTF) competition style is a successful way of introducing students to various technical concepts in the standard computer science curriculum. During the 2019 school holiday, a CTF for secondary school students was conducted at Universiti Tenaga Nasional (UNITEN) with the primary goal of introducing secondary school students to various cybersecurity topics and also to inculcate their interest in cybersecurity. We used a scenario-based approach that also took into account the syllabus for Malaysian secondary school. We found that this method attracts participants in solving each challenge in a competitive environment.**

Keywords – Cybersecurity, Capture the Flag, Game, School students

I. INTRODUCTION

Since 2017, the Malaysian education system has integrated computer science in the secondary school curriculum through the Standard Based Curriculum for Secondary Schools (KSSM). This implementation is seen as a great initiative to increase the number of students with computer science skills. At the same time, it contributes to more potential computing professional resources in the future.

However, statistics show a steady drop in student enrolment in the Science stream at the secondary school [1]. Also, the quality of STEM (science, technology, engineering, and mathematics) graduates is very worrying, with more than 48% of Sijil Pelajaran Malaysia (SPM) candidates failed to obtain a Credit grade of C for Additional Mathematics. Since most of the pre-requisites for enrolling in cybersecurity courses at the university are a credit in the subject of Additional Mathematics in SPM, this also limits the selection of cybersecurity courses at the university level among school leavers.

This situation is not just happening in Malaysia. Indeed, there has not been a significant increase in the proportion of Americans who are studying in STEM majors in the past years [2]. In Hawaii, business leaders unable to find STEM talent they need to stay competitive [3].

A study [4] conducted indicates that providing students with a high school context that offers a greater number of STEM courses, more information regarding STEM careers, and a large percentage of peers interested in STEM is not enough to ensure students' STEM-related college outcomes will improve. Instead, various individuals, families, and prior educational dynamics show a higher likelihood of enrolling in STEM majors in colleges.

Raising awareness among students, educators, mentors, and parents on career opportunities for cyber professionals is important [5]. Laurin Buchanan highlighted that "Kids don't say "I want to work in the medical profession when I grow up." They say, "I want to be a doctor, a nurse, a sonogram technician, an EMT." They pursue specific roles that they have seen and understand what is involved that they know who is helped by that person or that role. In the cyber arena today, there is almost no visibility at this level."

As secondary school students spend about five years in the school, the school can be the avenue to expose cybersecurity to the students [2]. This may be a new field for them to understand since they may have only read about it or heard about this field on the news or elsewhere in the media. Hence, this could be an opportunity to inform them and provide information on the program and prospects for a career in cybersecurity.

However, one study showed that teachers' level of understanding and self-ability to teach cybersecurity subjects is still low, causing teachers to be unprepared to teach cybersecurity-related subjects [6]. Due to this issue, there is a possibility that fewer students know about cybersecurity. Consequently, all educators are expected to have a general working knowledge of cybersecurity [5][7].

This situation may also contribute to the inadequate of skilled cybersecurity professionals to deal with a growing number of attacks [8]. With the increasing number of attack tools available and the evolving cybersecurity threats, and the declining of Science streams enrolment at

schools, Malaysia might suffer to cope with the huge demand in the cybersecurity domain [9][10]. This issue was also highlighted by CyberSecurity Malaysia chief executive officer, Datuk Dr. Amirudin Abdul Wahab [11]. Therefore, it is crucial to look at the initiative to broaden participation and interest to inculcate a STEM mindset, especially cybersecurity among secondary school students in Malaysia.

In preparing modules or learning materials to introduce cybersecurity to students, a common way to deliver is PowerPoint slides, textbooks, academic articles, and many more. Together, educators use various assessment tools to evaluate student's performance; examples are assignments, quizzes, and exams. While for practical sessions, educators might use the lab materials to conduct the sessions.

Alternatively, educators may consider various options [12], [13] to deliver their teaching materials. For cybersecurity-related topics, a competition is organized to get students interested and involved in cybersecurity, known as Capture The Flag (CTF) [14]. By using this platform, students will be presented with a set of challenges that test their creativity, technical skills, and problem-solving ability.

In this study, CTF competition is expected not just for teaching valuable skills but also for secondary school students in Malaysia to gain excitement about computer science and cybersecurity. At the same time, it might also raise their awareness of cybersecurity issues and later may inculcate their interest in cybersecurity.

II. Reviews on CTF Topics and Secondary School Syllabus

A. *Various Capture The Flag (CTF) Topics*

CTF competitions can involve Jeopardy-style questions or hands-on Attack-Defense activity on a network [15][16]. Teams competing in the battle for Jeopardy are required to exploit the services provided by administrators. The participants were only involved in the attack, and administrators provided only a few services. Teams are focused on leveraging as much vulnerability as possible.

However, in Attack-Defense, each squad has its own PC under command, all of which have the same services. The players are in a position to defend the services available on their PCs and at the same time try to disrupt the services available on the opponent's PCs. To do so, groups are tracking flag stealing vulnerabilities in systems (and their source code). If a vulnerability is found, a team can resolve that failure in its programs and build a tool to take advantage of the limitation in the services installed on all PCs on the other teams. A good feat leads to flag theft, which can be exchanged for points.

Most CTF competitions organized outside Malaysia are usually offered for adult professionals, undergraduate students, and high school students. Participants learn about cybersecurity concepts while having fun answering questions in such categories as cryptography, forensics, web applications, and reverse engineering.

CTF competitions can be viewed by many as a channel to attract students to STEM fields and to stimulate creative thinking and innovation through intellectual problem-solving among secondary school students. Examples are PicoCTF [17], CTF Unplugged [18], Maryland Cyber Challenge [19], CyberFirst Girls Competition, CyberPatriot [20], and MITRE STEM CTF [21].

PicoCTF is a web-based free security game designed by Carnegie Mellon CyLab, for mid-to-high school students [17]. The game consists of a set of challenges based on a common context, including players in reverse engineering, cracking, hacking, deciphering or doing anything they can to overcome the problem. Both tasks were created in order to be cracked, rendering it an ideal and legitimate way to obtain practical experience.

Tennessee Tech University CTF [18] is the best example of a program in which participants with little or no awareness of the various challenges faced by cybersecurity practitioners. At the event, participants were exposed to problem-solving abilities in cybersecurity, primarily learned during the Tennessee Tech University GenCyber School. After attending the event, students reported significant gains in comprehension, confidence, and comfort.

Capture the Talent by the Unitec Institute of Technology of New Zealand [22] is another CTF competition worth mentioning. This competition was developed specifically in order to try and become the stage for cybersecurity awareness training in New Zealand. This initiative gives high school students the opportunity to participate in a challenge to solve actual cybersecurity issues by hacking, pattern recognition, and the implementation of innovative and critical thinking processes. It is the first competition like this because it went beyond the curriculum and was focused primarily on high school students in New Zealand.

In Malaysia, CTF competitions are only open for undergraduate students. Examples are Cyber Heroes Competition [23], F-Secure Intervarsity Cybersecurity Competition Malaysia [24], and HACK@10 2018 [25]. The competition hosted in Malaysia is suited for undergraduate students to demonstrate skills and for hiring managers from the industry to identify the best resources with the best skills.

For this study, we decided to use the same approach as Chapman and Brumley [26] and Deylami *et al.* [27] whereby a scenario was built and a CTF situation that correlates with the scenario was designed in order to create a more immersive and beginner-friendly CTF competition.

B. Secondary School Syllabus

From our review in Malaysian school syllabus as of 2019 based on computer science stream in secondary school's textbooks "Basic Computer Science" for lower secondary (age 13-15) and "Computer Science" for upper secondary (age 16-17), we found out that for computer science stream students in secondary school, most of the syllabus consists of programming, algorithm and problem-solving. Starting from the age of 13 (Form 1 students), they were taught fundamental problem solving, data representation, and pseudocode algorithms.

As they proceed in their academic years, they learn more complex topics, but still, most of them are geared towards a programming-related topic such as learning to code in C, Java, HTML, and Python. This can be proven whereby starting from the first year until their last year in secondary school (Form 5), they constantly learn algorithms and problem-solving.

C. Security Related Topics for Secondary School Syllabus

The review of topics for secondary school syllabus is based on Malaysian secondary school coverage. In terms of cybersecurity topics, the students are exposed to basic ciphers such as Caesar cipher, substitution, Pigpen, rail fence, and transposition cipher during Form 3. In the Form 5 syllabus, cybersecurity-related topics are introduced, such as symmetric and asymmetric encryption and cyber forensic law and policies. This shows that only a small number of cybersecurity topics are exposed to students, and it does not provide the opportunity and space for those students to be interested in cybersecurity.

In this study, topics on cryptography and forensic were included due to the student's understanding of the cryptographic technique used in computer science and a certain level of digital forensic knowledge. We believe such an approach can be a fun way to attract this student in taking the cybersecurity-related field in the future since playing with cryptography is basically playing with a puzzle, and the sense of achievement in decoding the ciphertext can be very rewarding.

III. UNITEN CYBER HUNT

On 14 December 2019, UNITEN organized and conducted5 the first cybersecurity competition for secondary school students, called UNITEN Cyber Hunt. This event includes a series of workshops and hands-on exercises for students between the age of 15 and 17.

The primary goal of this event is to inculcate interest in cybersecurity and to educate secondary school students about technical knowledge in cybersecurity. The exposure of the CTF competition to them is expected to help build their confidence to participate in similar events in the future

A. CTF-based Scenario Development

The scene was conducted in a 4-parts story scenario where the participants were considered forensic investigators in training and help to solve a murder crime. The rundown for each scenario is shown in Figure 1:

Figure 1: CTF-based Scenario Flow

1) Trainee Recruitment: The scenario starts with the recruitment stage of the forensic investigator trainee. In this stage, the participants were required to mingle around and solve multiple activities that we considered as an ice-breaking session during a more typical event. We decided to include this ice-breaking session as the start of the scenario in order to better simulate and enhance their immersive in the gimmick we about to run. This was done in order to not only help the participants socialize with fellow participants but also to help them build teamwork via fun activities.

2) Forensic Training: The written part of the scenario was where the CTF workshop happen. It consists of 4 stages of the workshop; Cryptography, Steganography, Web and Forensic as shown in Figure 2.

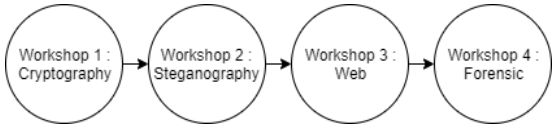

Figure 2: Scenario 2 flow

In this stage, the participants were given a "forensic investigation training" that was actually a collection of CTF training workshops with multiple topics which consists of cryptanalysis, web investigation and problem-solving. We also, however, include a few new topics that were not included in their syllabus and a practical tool usage scenario for forensic investigation such as steganalysis and forensic investigation. The topics are included because there are some questions in the actual CTF that will use the tools. A few sample challenges were designed and used in order to help them better understand the topics.

3) Crime Scene Investigation (CSI): For the next part, we decided to create what we called a crime scene investigation gimmick in order to teach them digital evidence acquisition and also expose to them to one of the branches of cybersecurity career which is a First Responder and Digital Forensic Team. The flow of the scenario is shown in Figure 3.

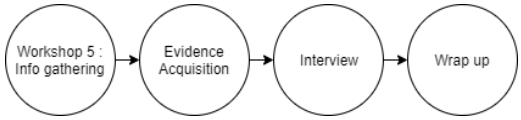

Figure 3: Scenario 3 flow

4) Forensic Lab: In this final scenario, the evidence gathered from the previous scenario is used in conjunction with the given case file. At this stage, the CTF competition officially began, where participants had to complete the CTF challenges using the tools and knowledge they had learned during Scenario 2. The challenges were designed for the students to use everything they learned during the day and apply them. The team with the highest points is awarded a reward.

B. CTF Challenges Development

In the CTF competition, the students look for hidden data in pictures and file systems regarding forensic challenges. The cryptography challenge requires students to decode text messages that are encrypted with both classical and modern authentication methods.

In the web challenges, students were introduced to simple HTML and PHP applications and had to use common techniques like Source Inspection and basic page directory in order to get the flag. The challenges were designed to encourage students to learn technical skills and practice them in addition to the traditional high school curriculum and uncover the mystery and found out the truth of the murder case scenario.

For the information-gathering questions, the participants are given a page of information, a case file describing the criminal, Jigsaw. They are then required to extract meaningful information that may or may not help in the investigation. This question aims to introduce the participants to the basics of forensics and information gathering.

The challenge only requires the participants to read through the presented data of a forensics scenario and find information to answer the question. The case file states that the computer from the crime scene displays a blank web page in which the participants need to investigate further. HTML is a part of the education syllabus. We would like the participants to feel as though they are applying what they have learned in school to feel more engaged in the event and not just learn new things.

Multiple steganography questions were also designed to retrieve an image file and show a person that might be Jigsaw. Participants need to apply their steganography skills to investigate the image. When it comes to digital forensics, the student curriculum and syllabus only exposed them to the rules and guidelines and also the law part of digital crime and evidence but never any practical exposure. This will mitigate that problem and also introduce them to steganography and steganalysis used in digital forensic. Even though we only touch a little bit on steganography due to its harder challenges and complexity in other CTF competitions, this will help them understand its basics.

There were several challenges explicitly designed for forensic and cryptography topics. For digital forensics, physical evidence which in our case the test file that they received earlier, was crucial information that is helpful when it comes to solving or understanding clues at the crime scene.

We designed the competition this way to teach them how the evidence can be chain together and be of use in the latter part of the investigation. As for cryptography, this challenge can help us to educate them about secure communication but in a more practical matter. This helps them understand more specific topics and broadens their thinking in terms of how we can apply such methods in our daily lives as we interact and how dangerous and easy it is for people to deny what is right in front of them.

C. CTF Challenges Scenario Development

Firstly, we designed the CTF competition by providing the participant with a scenario to help them better understand their role and motivation for doing the challenges. This helps grab the participant's attention and provides them with a fun simulation of being part of a digital forensics team. This approach was chosen based on research done in PicoCTF [24] where they chose the educational CTF approach via scenario cases which was "Toaster War" and in order to better accommodate newcomer mentality and skills set to not only teach them CTF beginner style but also to help CTF newbie in learning in a more user-friendly environment and grabs their attention. Based on the success that follows PicoCTF, we decided to follow the same approach and provided the scenario. We then gave them a number of prepared items or, as we called them 'case file' and set up a crime scene to help them in their competition. The items given were as follows:

(i) 1 page of information about the killer such as past cases that have clue related to the latest crime.

(ii) A USB drive with 5 types of evidence. Zip file with a group photo of victim with GPS location data, .docx document with a paragraph of messages, .xls document which include bank ledger balance, .txt document with a binary number and lastly 3 RGB colour.

Table 1: Overall Achievement of 16 Teams

Challenge	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7	Team 8	Team 9	Team 10	Team 11	Team 12	Team 13	Team 14	Team 15	Team 16
1	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
2	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
3	P	P	P	P	P	P	P	P	P	P	F	P	P	P	P	P
4	P	P	P	F	P	F	P	F	P	P	F	P	P	P	P	P
5	P	F	P	F	P	F	P	F	P	P	F	P	P	P	P	P
6	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
7	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
8	P	F	P	P	P	P	P	P	P	P	P	P	P	P	P	P
9	P	F	P	F	P	F	P	F	P	P	F	P	P	P	P	P
10	P	F	F	F	P	F	P	F	P	P	F	P	P	P	P	P
Secret	P	F	F	F	F	F	F	F	P	P	F	F	P	P	F	F

P: Passed the challenge
F: Failed the challenge

This scenario has been used throughout the competition in order to capture participants' interest and provide them with a real-life simulation of evidence investigation gimmick.

IV. Analysis and Findings

By the time the competition was over, five teams had succeeded in solving the crime, but only one team had succeeded in finding the motive of the whole crime scene scenario. Here are some assumptions:

1. The participants did not read the questions thoroughly for the hints in the challenges.
2. The participants struggled to use the proper tools or commands for specific questions.
3. Failed to find the pattern that is associated with the challenges questions.

Table 1 shows the tabulated data on which team managed to complete which challenge during the event. "P" means that they managed to complete the challenge, while "F" means they failed to complete it.

1) Challenge 1

These information-gathering questions for this scenario can involve either a physical copy or a digital copy of the question. The participants are given a page of information on the case, a case file that describes the criminal, Jigsaw. They are then required to extract meaningful information that may or may not help in the investigation.

This question aims to introduce the participants to the basics of forensics and information gathering. The challenge only requires the participants to read through the presented data of a forensics scenario and find information to answer the question. Evidence acquired from this challenge will be the killer's email address. All teams completed this challenge without any issue. During this challenge, the only problem was the fact that false flags were submitted even though it was the correct word due to incorrect flag format.

2) Challenge 2

The next information gathering question continues from the previous challenge. The case file states that the computer from the crime scene displays a blank web page in which the participants need to investigate further. The HTML file contains a hidden image that is used for the next steganography question. Participants will have to inspect the element of the blank HTML page and download the image file. HTML is a part of the education syllabus. We want the participants to feel as though they are applying what they have learned to feel more engaged in the event and not just learn new things.

Evidence acquired from this challenge will be an image of a person leaving the crime scene. All teams completed this challenge without any issues. The only problem faced by the participants was that most of them overlook the file name for the flag, while some forget to download the picture first before obtaining the flag. None of the participants has an issue using the web inspector that was being taught during Scenario 2.

3) Challenge 3

The next question continues from before. An image file is retrieved which shows a person that might be Jigsaw. Participants need to apply their steganography skills to investigate the image.

The image file contains a password to access the email. Participants will have to use strings to check for the hidden information and find out the method by which the information can be extracted. The clue in the string is '*steghide*' encoded in base64, which meant the participants have to use '*steghide*' tool to extract the information hidden in the image. The evidence acquired is the password for accessing the email.

Out of 16 teams, only 15 teams managed to complete this challenge. The program facilitator discovered that the unsuccessful team was unable to identify which tools to use for this challenge since the hint will only appear after they issued the strings command. The team also was having trouble with the '*steghide*' command line and appended the wrong command option.

4) Challenge 4

The next steganography question continues from the previous question. A .png image file is extracted from the email folder and contains some text that might be crucial to the case. But, is the information correct? Participants need to investigate more.

They are required to check the spam folder of the email and download the image attachment. There is information for a file called 'secret.png' and 'global.png' using a string command. The participants are requested to use the '*binwalk'* tool for finding and extracting the hidden files. Then, extract the hidden files using '*binwalk'*. Evidence acquired is a photo showing the company inventory.

Only 12 teams managed to solve this challenge. Based on an impromptu interview with the unsuccessful teams, the main issue for them was that they failed to identify the correct tools to use. Most of them used *'stegsolve'* to solve this challenge. The hint given was also very confusing to them, considering how they did not understand the pun on the name '*binwalk'*. Clarification on the hint and question should be revised for the next iteration of the study.

5) Challenge 5

This question uses one of the images that had been extracted from the previous question, which is the "global.png". The purpose is to show the participants how information can be hidden in an image bit plane as taught in Workshop 2 (Scenario 2).

This question is separated into two parts. The first part is the hint by looking at the metadata of the image using *ExifTool*. The second part is the flag. Participants can use '*stegsolve'* or site online to look at bit planes where the flag hid. Evidence acquired is the killer's signature logo with hidden taunting text.

For this challenge, 11 teams managed to complete it. The reason for the unsuccessful attempt by the other five teams was due to the following reasons:

i. Since the question was linked to the previous question, four teams failed to access this question due to incomplete pre-requisite requirements.
ii. One team did not manage to find the second flag, which is the true flag hidden inside the picture bit plane, and submitted the flag for the last question since both flags were on the same file.

6) Challenge 6

For this question, we have used an audio file. The purpose is to show participants that steganography is not applied to image only. We also wanted to test them on one of the topics frequently being challenged in many CTF competitions.

Participants need to use audacity or any other related audio waveform software and check the audio file spectrogram to get the flag. Evidence acquired is a hidden text in voice recording.

All teams managed to submit the flag for this question. This might be due to how keen they are in listening and trying the examples for this type of question in previous Scenario 2. This was also the topic that piqued their interest in Audio Steganography and was voted the most interesting by the participants unofficially.

7) Challenge 7

For this challenge, the participants were required to check the .txt document for the zip file password. The text file contains ten binary numbers, with only one of them translated to a proper ASCII character. They need to do this via a basic binary translator. Evidence required is the date of murder for each victim.

All teams managed to submit the correct flag. The reason for this was due to how direct the question being asked and how easy the process to decode was. However, submission of the failed flag for this question was the highest where out of 63, 47 failed flag submission was registered, due to the date format being inputted wasn't the correct format of DDMMYYYY. Most of the flag received in the system was in DDMonYY.

8) Challenge 8

Steganography and basic Linux command line were merged and were chosen as the next challenges due to the simplicity and easiness and also how mainstream the challenge is in CTF competition.

The participants were required to open a .zip file. The .zip file they open will contain a group photo that contains the victim's face and killer face within those groups. The photo will hide two things, the key, and the GPS location. The key will be retrieved via the basic unzip command in the Linux terminal, but that is only one part of the key. The 2nd part will be inside the file itself, whereby by changing the extension from .png to .zip they can extract a .txt file that contains information about the hint.

From the hint, participants had to extract information by examining the metadata of the .png file, including the GPS location of the photo. The group that obtained the GPS location information will successfully pass this challenge.

9) Challenge 9

We decided to enhance the participant's understanding of evidence digging for this challenge, but this time we introduce a more common file, an Excel file. With the same goal as the previous inclusion of forensic elements as challenges before this, we assume that the participants are quick-witted on what to do next after discovering the hint of earlier challenges. The file contains a lot of money in and out of records. This time the key will be found in the spreadsheet metadata as hidden text, but there will be two pieces of information. One is the flag, and another one will be a URL. The flag can be found by changing the file extension to .zip file and go through each file's content.

Only 11 teams managed to complete this challenge. The reason for the other five teams unable to complete this challenge was due to these factors;

1. It is a chain question. The pre-requisite challenge was not completed by one team.
2. Difficult to find the flag in the zip version of the spreadsheet. They did not know that by opening

the spreadsheet and press Ctrl+A, and then changing the font to black could also reveal the flag.

3. Failed to find the hint since the hint can only be accessed after checking the column corresponding to the last question flag, column 7G and 7C.

10) Challenge 10

For this semi-final question, we decided to develop it to look like the final question to confuse the participants. The web server can be accessed through the URL found in the previous challenge. We also included other open-source tools to see if they still remember the things they learned in Scenario 3 for Information gathering. The question was also design with multiple HTML page navigation to see how the participants handle repetitive page directory navigation and see if they were persistent enough to find the 2nd last page for the flag. They only need to perform basic webserver navigation with simple web page source code inspection.

The webpage accessed from the URL found in the previous challenge contains a fake error message and contains the hidden text of the number in the source code. The webpage source code will contain an RGB number which if they input into 'http://www.telacommunications.com/cgi-bin/rgb.pl', they will receive the hex value. This hex value will be crucial as it will be the page directory when entering the web browser URL. After they navigate to the right directory, they need to check the page source file, giving the flag. Evidence acquired will be a secret message inside the webpage source code.

For this challenge, 10 teams managed to complete it. The other 6 teams did not complete it due to them not being persistent enough to navigate the whole web server repetitive action. Some of them even failed to find the correct HTML page due to them skipping the process to translate the RGB color given into Hex and navigate to that hex value page. Some were even confused as to what needs to be done after the first page navigation.

11) Secret Challenge

This challenge was developed to decide who is the winner for the top 3 places. Only those who are interested to dig deeper into the webserver directory may find this page. This challenge was also created to be the final link in the whole crime story and to figure out the motive and the desperation of the killer to hunt all his victims. We decided to include Linguistic Steganography to introduce them to another type of steganography.

The final challenge is a continuation of the last challenge. If they navigate to the page directory with the last flag as the keyword for the directory, they will stumble upon another page with base 85 encoded text in the hidden text of the HTML page. After they decode it, they need to check every 5th letter of the text to find the real meaning behind the letter. It will show who tells who to murder who. The crucial evidence found is the motive and an order to kill a letter from someone.

For this challenge, seven teams managed to find the challenge, but only five managed to complete the challenge. The pre-requisite for accessing this challenge is to complete all 10 previous challenges, and since only seven of those teams managed to pass this pre-requisite, the results are understandable. However, out of five teams, only one team manage to decode the Linguistic Steganography and find out about the motive of the killing and who is the conspirator.

During the whole case, cybersecurity knowledge was gained in several ways. A new form of CTF competition was introduced that is based on a written scenario. The participants were given a CSI Detective Role and Training Laboratory session before the competition, in which they would have exposed themselves to the competitive cybersecurity scene. There were two specific issues in the pre-test, and post-test questionnaire, which are meant to search for differences before and after the UNITEN Cyber Hunt event.

Table 2. Comparative analysis of pre-test and post-test

Questions	Average rating/percentage	
	Pre-test	Post-test
Participants are interested in cybersecurity.	3.90	4.09
Participants plan to pursue opportunities to learn about cybersecurity.	34.4%	21.9%

As shown in Table 2, the participants' involvement in cybersecurity will easily be strengthened if properly managed. The number of participants who were interested in cybersecurity rose by 12.5% after the study. Nevertheless, the number of participants planning to take chances to gain a better understanding of cybersecurity has decreased slightly. It may be due to some challenges that are quite difficult to solve. Although some learners, who tend to be more capable relative to others, have managed to keep pace, most of them consist of students who are in lower levels. These students may not have been prepared for such technical challenges, especially those who are completely unaware of cybersecurity.

V. CONCLUSION

UNITEN Cyber Hunt was a great learning experience both for the students involved and for the organizers. Based on the results shown in Table 1, this CTF scenario-based approach has shown how current computer science would be enhanced by adding cybersecurity topics and more CTF competitions for secondary school students.

From the organizer's perspective, CTF style highlighted the participant's strengths and weaknesses and explained topics that they do not understand much at the end of the competition. Teachers can see the same perspective as they can see student performance more easily and can identify which topics need attention.

For future improvement, we will be conducting a series of CTFs for secondary school students by focusing on one cybersecurity topic to see the effectiveness of CTF and student understanding of the topic.

ACKNOWLEDGEMENT

This study was funded by BOLD 2025 Universiti Tenaga Nasional (10436494/B/2019079). We would like to thank UNITEN Innovation & Research Management Centre (iRMC) for fund management.

REFERENCES

[1] The Star Online, STEM literacy for industry 4.0, 2018.

[2] M. C. Bottia, E. Stearns, R. A. Mickelson, and S. Moller, Boosting the numbers of STEM majors? The role of high schools with a STEM program, Sci. Educ., vol. 102, no. 1, pp. 85–107, 2018.

[3] D. Nakama and K. Paullet, The Urgency for Cybersecurity Education: The Impact of Early College Innovation in Hawaii Rural Communities, Inf. Syst. Educ. J., vol. 16, no. August, pp. 41–52, 2018.

[4] E. Glennie, M. Mason, and B. Dalton, The Role of STEM High Schools in Reducing Gaps in Science and Mathematics Coursetaking: Evidence from North Carolina. Research Report. RTI Press Publication RR-0025-1603, 2016.

[5] Katzcy Consulting, Cybersecurity games: Building tomorrow's workforce, 2016.

[6] P. Pusey and W. A. Sadera, Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference, J. Digit. Learn. Teach. Educ., 2011.

[7] S. Furnell, P. Fischer, and A. Finch, Can't get the staff? The growing need for cyber-security skills, Comput. Fraud Secur., vol. 2017, no. 2, pp. 5–10, 2017.

[8] M. J. Cobb, Plugging the skills gap: the vital role that women should play in cyber-security, Comput. Fraud Secur., vol. 2018, no. 1, pp. 5–8, 2018.

[9] J. Jacob, W. Wei, K. Sha, S. Davari, and A. Yang, Is the NICE Cybersecurity Framework (NCWF) Effective for a Workforce Comprised of Interdisciplinary Majors?, in International Conference Scientific Computing, 2018, pp. 124–130.

[10] M. E. Armstrong, K. S. Jones, and A. S. Namin, Framework for developing a brief interview to understand cyber defense work: An experience report, Proc. Hum. Factors Ergon. Soc., vol. 2017-Octob, pp. 1318–1322, 2017.

[11] R. Sani, What it takes to become a cybersecurity specialist, New Strait Times, 18-Jul-2018.

[12] F. Y. Al Irsyadi, Supriyadi, and Y. I. Kurniawan, Interactive educational animal identification game for primary schoolchildren with intellectual disability, Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 6, pp. 3058–3064, 2019.

[13] M. G. Sergeeva, N. L. Ogurechnikova, G. V Zarembo, N. V Nikashina, E. V Nagornova, and E. A. Baranova, Methodology Development of the University Teacher's Creative Abilities with the Help of Information Technologies, Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 6, pp. 2800–2805, 2019.

[14] J. Umawing, Engaging students in cybersecurity : a primer for educators, Malwarebytes Labs, 2018. [Online]. Available: https://blog.malwarebytes.com/101/2018/05/engaging-students-cybersecurity-primer-educators/.

[15] S. Wi, J. Choi, and S. K. Cha, Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competition, USENIX Work. Adv. Secur. Educ., vol. 1, pp. 1–9, 2018.

[16] R. Raman, S. Sunny, V. Pavithran, and K. Achuthan, Framework for evaluating Capture the Flag (CTF) security competitions, 2014 Int. Conf. Converg. Technol. I2CT 2014, pp. 1–5, 2014.

[17] Carnegie Mellon University, picoCTF, 2019. [Online]. Available: https://picoctf.com/.

[18] V. Ford, A. Siraj, A. Haynes, and E. Brown, Capture the flag unplugged: An offline cyber competition, in Proceedings of the Conference on Integrating Technology into Computer Science Education, ITiCSE, 2017.

[19] Federal Business Council Inc., Maryland Cyber Challenge, 2019. [Online]. Available: https://www.fbcinc.com/e/cybermdconference/challenge.aspx.

[20] Northrop Grumman Foundation, CyberPatriot, 2019. [Online]. Available: https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx.

[21] The MITRE Corporation, MITRE STEM CTF, MITRE Cyber Academy, 2019. [Online]. Available: https://mitrecyberacademy.org/competitions/index.html.

[22] H. M. Deylami, M. Mohaghegh, A. Sarrafzadeh, M. McCauley, I. Ardekani, and T. Kingston, Capture The Talent: Secondary School Education with Cyber Security Competitions, Int. J. Found. Comput. Sci. Technol., vol. 5, no. 6, pp. 55–66, 2015.

[23] CyberSecurity Malaysia, Cyber Heroes Competition 2019, 2019. [Online]. Available: http://www.cyberheroes.my/.

[24] F-Secure, F-Secure Intervarsity Cybersecurity Competition Malaysia, 2019. [Online]. Available: https://bit.ly/FSCompetition2019.

[25] Universiti Tenaga Nasional, HACK@10 2018, 2018. [Online]. Available: http://hack10.uniten.edu.my/.

[26] P. Chapman and D. Brumley, picoCTF : Teaching 10,000 High School Students to Hack, 2013.

[27] M. Ricci et al., Framework for evaluating Capture the Flag (CTF) security competitions, Usenix, vol. 5, no. 4, pp. 5479–5486, 2016.