A STEM and gamification approach: CTF for undergraduate students

Daniel Altman
altmand2@mail.sacredheart.edu
Akshay Kumar Mandlem
mandlema@mail.sacredheart.edu
Rex Sprosta
sprostar@mail.sacredheart.edu

Submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Cybersecurity

Sacred Heart
UNIVERSITY

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

School of Computer Science and Engineering
Sacred Heart University
May 18, 2024

Abstract

Cybersecurity is a topic that is a crucial aspect in modern times. Being part of one of the STEM disciplines aims to use a blended model as part of the approach, integrating traditional education (theoretical) with hands-on exercises, giving the students a more immersive experience. As Joseph Feiman stated in an article: "In an increasingly complicated world, success is achieved not just by the things we know, but by what we can do with what we know" [1]. In thinking about this approach the concept of gamification is viewed as a modern way to teach. It's a tool to engage students in learning. Additionally, in a world where technology is enhanced and/or developed every day, the need for protecting sensitive information is imperative. Obtaining the knowledge on how to protect data is imperative for an individual or businesses as a whole. The understanding of how data and other sensitive information can be exploited is key. The impact that this could possibly have on daily activities can bring Cybersecurity to the forefront. It is an issue that should be taken seriously by every user, not just Cybersecurity professionals. A hands-on CTF blend between Jeopardy style and red teaming exercises approach for students seeking to work in the Cybersecurity industry serves as a great opportunity. The demand within the field has an expected 13.8 % annual growth rate between 2023 and 2030[2].
Keywords: *CTF, hands-on, Cybersecurity, Ethical hacking, Educational, Undergraduate Students*

Contents

Chapter 1

Introduction

Computers have always been a tool that enables enhanced teaching and learning by hands-on experimentation and it has become one of the pillars of the STEM approaches narrowing to Computer Science by "Expanding Digital Platforms for Teaching and Learning"[3]. As it's main purpose is to create scenarios that can transcend basic approaches for teaching and learning and get full benefits of the digital technology based learning environments. It's known that new attack vectors are being used against every user or business sector. However, there is a large percentage of end users that are still using old technologies or software that are not secure or completely outdated, so it's not absurd to teach from the basic concepts of security. As part of this initiative there have been countless science fairs, math contests, invention challenges, mathematical gaming, and cybersecurity contests among which we can encounter CTF based challenges with multiple levels of difficulty going from beginners covering just the basics to experts who can perform more complex and diverse tasks and challenges.
CTF challenges brought profound changes to the way that cybersecurity is being taught. These types of exercises started to integrate puzzles, challenges and real-world scenarios that are demanding of more problem-solving skills, teamwork, critical thinking and analytical skills. This in turn made the educational scenarios more of a revolutionized approach allowing participants to experience active engagement, "victories" of real-world based environments. Students learned about either new or old trends, techniques, tactics and procedures -TTPs- that could help them moving forward.
CTFs nowadays have become really popular within the cybersecurity community and they can go from simple practice to worldwide competitions as cybersecurity isn't an issue in just one country or domain, but it is something that should concern every user that is willing to use a device connected to the internet.

The rise of CTF type of events has been such that at this point you can find a lot of them on internet. Some have incorporated cloud based events to increase the accessibility to them, challenges evolved to get more en-

gagement from the participants, real-world environments that makes the competitions more relevant within academic and workforce populations. In some instances there are prizes, sponsorships, media coverage and networking events, among others things that are making these events more professional and popular. Having this in mind, Capture The Flag (CTF) for undergraduate students aims to provide a platform with hands-on excercises for educational purposes that can be deployed in cloud or in local environments. The students can use the platform to sharpen their analytical skills, critical thinking, teamwork and problem solving skills. This immersive environment and experience will provide challenges to include cryptography and network security, reverse engineering and more. We aim to encourage students to dive deeper and accept the challenge to get a better understanding of the art which will aid them in the future to become more well rounded as cyber professionals.

Chapter 2

Literature Review

CTF(Capture The Flag) as a tool used in undergraduate courses at universities not only helps the instructors to identify students and their proficiency level but it also helps the students to learn and experience with hands on challenges. These challenges can be done in groups or individually throughout a semester depending on the structure and curriculum. The students have a chance to build and boost their confidence if they are not as experienced through repetition and friendly competition. The students can/will also benefit from the opportunity to collaborate and learn from their peers that may have some experience in the art. The underline goal is that they would learn from each other as the class progresses as they are introduced to different challenges. The professors would have an opportunity to review and examine the students through their hands-on work and based on the challenges that they were expected to complete during the course. This hands on approach could also help with quizzes and exams as the students would have to answer the challenges as best as they can based on the exercises that they have already experienced throughout the course."CTF games seems to be a better method in assessing of skills acquired during the semester, especially for large classes. Gamification features should bring students a more enjoyable learning experience, including not only technical but also teamwork. Instructors would benefit from automatic scoring of students submissions and not spend time consumed by the manual marking of student submissions more efficiently"[4] The CTF challenges would/could have a scoring and time element embedded as well.

Another CTF-based approach within teaching curriculum's was exposed by The United States Air Force Academy, that after participating and motivating students and teachers to be part of such events for 5 years decided to implement and develop a CTF-style curriculum with full credit courses going from large scale Jeopardy style to multi-day exercises style partnering with external entities. This approach was based on the necessity of exposing every students starting from freshman's to cyber concepts making emphasis in a defensive perspective focusing on topics like social engineering, malware and high-level vulnerabilities to national security allowing the students get a better comprehension through hands-on lab-

oratories that were intended to teach how attackers operate and from the victims side, how should they proceed. Even though the study was not conducted in a rigorous scientific manner, they have expressed that success was such that they " have seen obvious increases in student motivation, a willingness for more self-directed learning, and the desire to push their own boundaries for knowledge"[5].

In 2021 between the Department of Computer Science Virginia Tech and Center for Excellence in Teaching and Learning Virginia Tech wrote a report where the main idea was to explore the impact of incorporating CTF activities into co-curricular opportunities within Computer Science programs. The survey was conducted with 200+ student participants and was intended to emphasize problem-solving skills incorporating contemporary computer skill among multiple disciplines such as data science, cryptography, network security, among others through three different CTF-based scenarios. The CTF-based learning was built to be executed all along the term starting with concept and tips review to be preceded by hands-on challenges. By the starting of the term at least 94% of the students never heard about CTF's, about 70% had previous computing skills and 72% out of those reported that they just had experience of High School computing. However, as they moved thorough the course they quickly adapted to new topics and tools that allowed them to perform in such a way that by the end of it "demonstrated that students acquired comfort levels with the topics in a very short time. Contributing to the goal of students becoming more comfortable with computing experiences and cybersecurity concepts"[6]. After the challenges were over a survey revealed that 42% of all the students stated that this approach allowed them to comprehend and learn, raising self-improvement of 23%. From the perspective of the professors enrolled in the survey the process of creating studying material, preparing students and implementation of the study curriculum was low compared to what the students would learn. Most of them made progress improving their computer skills using the engaging, gamification concepts during their lectures making this scenarios more comfortable from the students perspective.

There are some inherent cons that come with capture the flag style hands on approach to teaching undergraduate students or any student for that matter. The most obvious issue is cheating. Just as much as the students would learn from each other collaboratively to help improve their skills, they could also cheat from each other while being assessed in any way. The instructor would also have a difficult time matching theory with the hands on approach. "Preparing CTF challenges for the hands-on part of an official exam can be difficult since the exercises must be tailored to the class's theory. This is precisely the opposite of what the author of challenges do: They aim to stimulate players to look for new solutions to unknown problems"[7].

The automatic evaluation of challenges is binary. Either the flag is correct, and the exercise gets the full credit, or it is wrong, and the exercise gets zero credit, no matter the quality of the partial solution. If this is acceptable for a competition, some care should be taken for an exam. Therefore, some strategies should be put into practice for a partial evaluation. One possible solution is allowing students, who did not find the right flags, to write their solutions (the writeups) immediately after the game. In this way, instructors can manually evaluate them and assign partial marks when possible"[7].

The next problem would be how to proliferate this across a broad array of subjects in Cybersecurity, from ethical hacking to networking to cloud computing. This would mean input from several different sources and disciplines would be imperative in order to customize this to the specific needs of each area or subject. While also attempting to match the theoretical portion of the course as required in most courses.

Chapter 3

Analysis

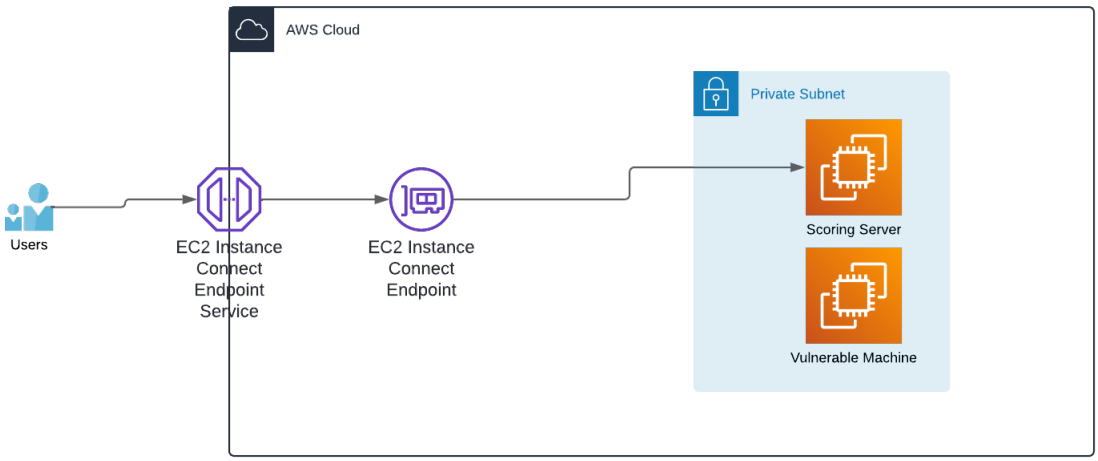
3.1 Cloud environment deployment

As part of the analysis for deploying this particular challenge and make it cloud based, we have explored Amazon Web Services[8] and configured it to remain in the free-tier features to ensure cost-effectiveness. The free-tier features that we are going to use within the platform is offered for new accounts and for the first 12 months as follows:

1. Up to 750 hours per month of Linux, Red Hat Enterprise Linux (RHEL), or SUSE Linux Enterprise (SLES) in t2.micro or t3.micro machines[9]. Scoring server and vulnerable box were developed using Ubuntu 22.04.4 LTS (Jammy Jellyfish) which will fit into this features.

2. 5 GB of Amazon S3 standard storage, 20,000 GET requests, and 2,000 PUT requests[9]. This one will be use to import the OVA machines into aws to deploy it later.

This features will allow us to deploy an engaging and challenging experience without incurring in expenses. The topography of this solution will be as shown in the image below:



This solution will allow up to 20 concurrent connections to the machines, so this scenario will host up to 20 singular students working by themselves or the same amount of teams focusing more in a team-working experience.

1. The scoring server pre-configured can be downloaded through this link: `https://drive.google.com/file/d/10ufa2yPcXW38x1WFQjxeq7T05ciIafas/view?usp=sharing`

User	Password
root	1234
ctfd	1234
admin	admin

   NOTE: The admin user is for the CTFd server to manage challenges and general configurations of the CTF.

2. The vulnerable machine can be downloaded through this link: `https://drive.google.com/file/d/1C-NmM3ijImKTjQWhDnNnKo_yox3brFfH/view?usp=sharing`

User	Password
root	1234
vuln	1234

3. A pre-configured Kali machine with all the tools and files needed to succeed along this challenge can be downloaded from this link: `https://drive.google.com/file/d/1O5VIeao9eSqWVpDDtBaHH34c4lamvEMK/view?usp=sharing` **NOTE: Advanced users may use another Kali box or OS of their liking.**

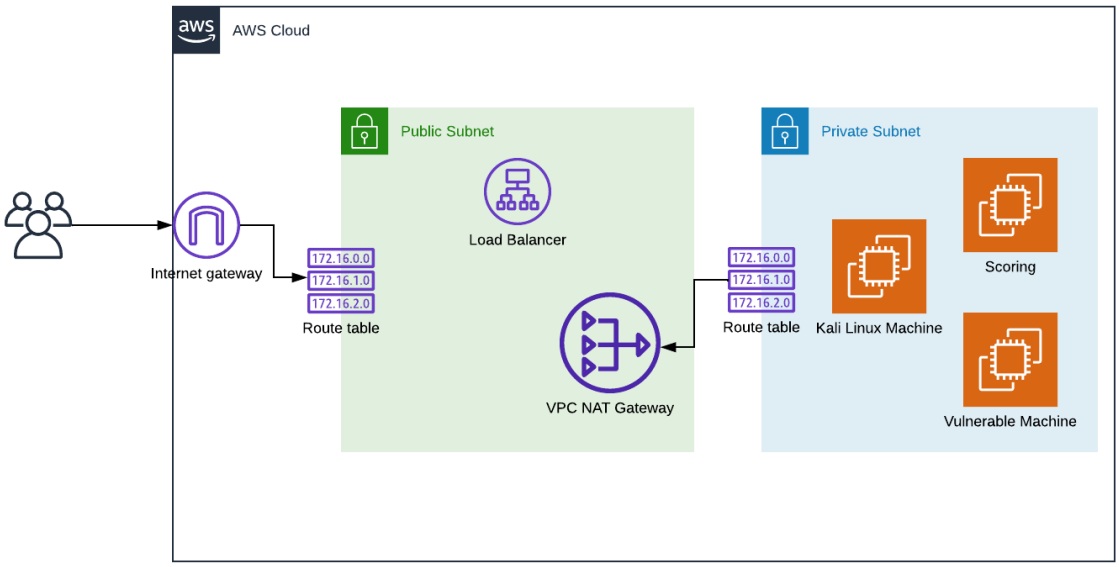
User	Password
kali	kali

4. The documentation including steps and commands to import the machines and convert them into Amazon Machine Image -AMI- and configuration can be downloaded through this link: `https://drive.google.com/file/d/1CAtxBO1KbszLpI6jahXgqMjDyRPahSUF/view?usp=sharing`

In order to support more concurrent connections to this scenario we will need to use another features that will have an associated cost as it will use different features from the ones included in the free-tier account. This additional features include the usage of public IP's and load balancer, configuring a more advanced setup that will adapt as users connect to the CTF challenge. The pricing for this two new features is detailed in the following chart[10]:

Service	Price/hour	Estimated Value
Elastic IP	$0.005	$0.02
NAT Gateway	$0.045	$0.18
Load Balancer	$0.0225	$0.09

So suppose a scenario where we are intended to host the event for about 60 students for 4 hours where they can connect to the scoring server and the attacking box (Kali Linux machine) with a smooth connection that will allow them to play around without any limitation. The setup for this will require at least 1 Elastic IP's (Public IPv4), 1 Load Balancer, and 1 internet gateway attached to it. This will incur expenses for about $0.30 cents.
For the previous described deployment the structure should look as the following chart.

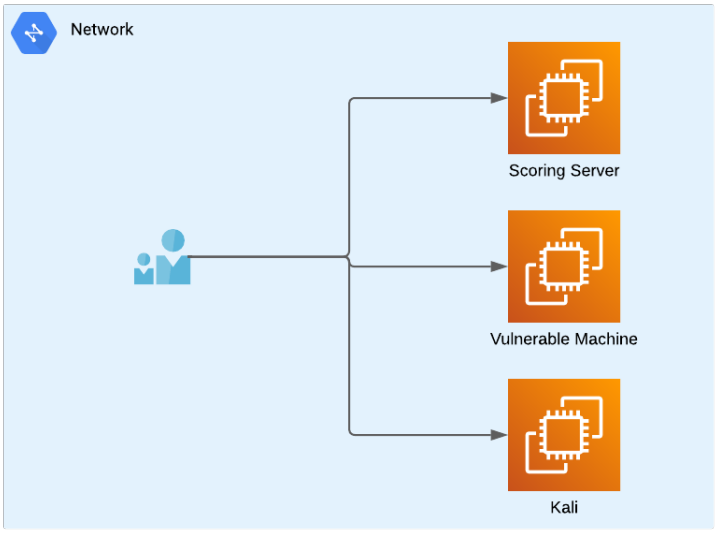


The step-by-step guide of how to deploy it and import the machines into AWS, with files required and detailed commands can be found in the following link: `https://drive.google.com/file/d/1CAtxBO1KbszLpI6jahXgqMjDyRPahSUF/view?usp=sharing`

3.2 Local

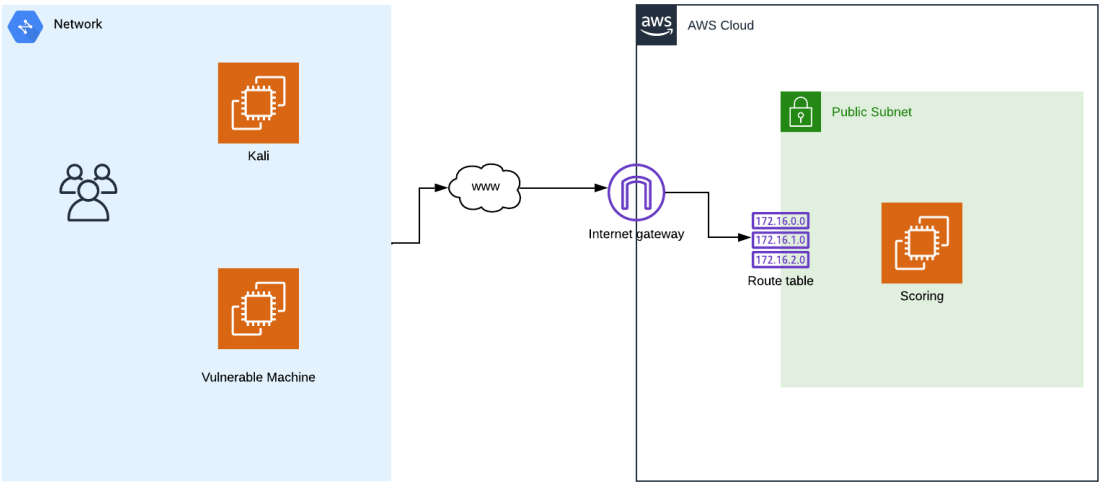
Deploying the challenge in a local environment will involve a few steps steps, such as importing the three machines provided in OVA format and can be imported to VirtualBox[11] or VMware[12] which are two of the most widely know open source virtualization software. Importing the machines won't assure that they are able to communicate with each other so networking is the next step during this process. We recommend use of the bridge adapter provided by local IP by the DHCP server. After checking that all the machines can communicate between them, you can access the scoring server by typing the IP address of the "ctfd" machine on port 80. The challenge by this time will be enabled and students can deploy the vulnerable machine in their own hosts, connect to the scoring server using any web browser of their preference and start playing around with the machine in which most of the flags are embedded, as some of them are focused on research so no interaction with the machines are required. This will limit the competency to be executed in Local Area Network (LAN).

The amount of concurrent connections in this scenario will vary depending on the resources available such as bandwidth but it will be more flexible as everyone will be using their own personal computer.



3.3 Hybrid

We have explored another way to deploy the environment that we suggest as the best choice. This still consist of deploying a machine in AWS (The Scoring Server) which can be done following the steps provided in the section 3.1 of this paper. For this particular deployment option we won't need EC2 instance connection devices and the vulnerable and Kali boxes can be obtained through the following link to be deployed locally: `https://drive.google.com/drive/folders/1AULkkW7kqRhNifBU6y8CPrsMU8aS1FVr?usp=share_link` **This will allow to execute the CTF while students are connected remotely and will provide more flexibility towards the development of the experience as it will allow up to thousands of concurrent users according to the concurrency policy of AWS.[13]**



Chapter 4

Implementation

4.1 Overview

4.1.1 Context

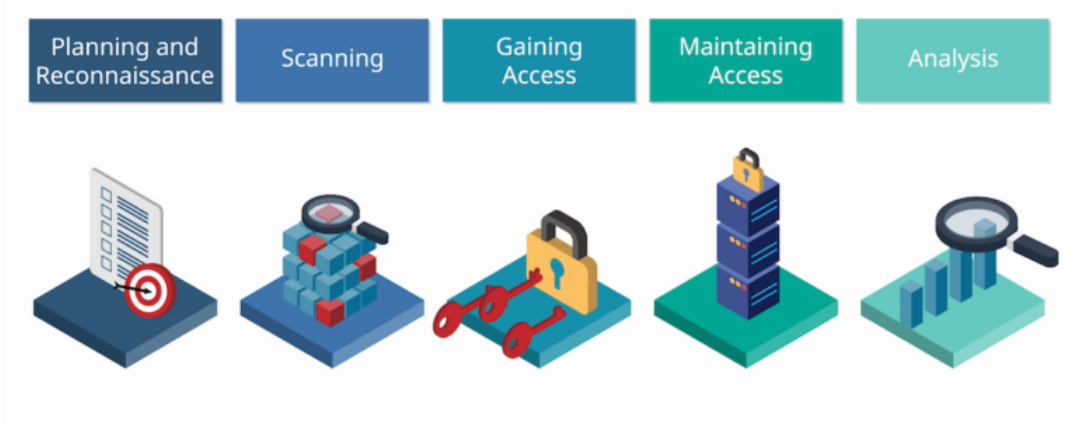
The CTF for undergraduate students was structured to be a successful blend between Jeopardy-style and Red Teaming "competition" to bring an engaging experience where students must complete 36 challenges that will cover basic to intermediate techniques in order to earn the badge. The challenges will cover topics starting from reconnaissance and going over critical security features such as cryptography, web application, forensics, network security and privilege escalation. The whole environment was developed to be able to play in a local machine or host it in Amazon Web Services platform. There is a scoring machine, a vulnerable machine in which all flags are embedded and a Kali Linux machine that will perform the role of the "attacker" as it comes with all the tools necessary to accomplish all the challenges. In the beginning of the competition, students will read over the "story" which will highlight some of the challenges ahead that will be available as they solve the problems working individually.

4.1.2 Exercise descriptions

All the hands-on challenges will have a flag that must be posted in the scoring server to confirm the correct answer, some challenges were set to have a max of three attempts but will not block you from moving forward. A brief description of the challenge follows.

1. **Warming up:** This is the first challenge the scoring server will make visible, it consist of a flag that has been obscured with Caesar's cipher and players will not be required to interact with any machine to accomplish the task. It provides a hint if they get stuck which will be free and when the task is completed, four more challenges will come to the table.

2. **Reconnaissance :** For the next four challenges, they will cover the Reconnaissance and information gathering concepts which will teach the first and the second stages of the pen testing cycle.



[14]

Within the four challenges the players must scan the network, obtain the vulnerable machine's IP, open ports and enumerate users.

3. **Cryptography :** For this domain players must decode a flag that have been obfuscated with an specific technique. On the other hand, a file has been encrypted using a password and the file with the key is provided. They must decipher the file in order to get the flag.

4. **Forensics:** Within this domain some files have been modified, embedding text, hiding files and changing the extension are the main tasks performed here. It's up to the students to find the tools and the right extensions to recover the flags.

5. **Network Security** : Players must find a network capture (pcap) file among the files in the system and they will have to examine it to acquire a file that is within the transference. After acquiring the file, they can find out the flag for this task. Then within the same capture and another pcap file within the system, they will have to find information related to protocols and IP's.

6. **Privilege Escalation** : Players must find a way into the machine that will allow them to connect to the machine as root. The flag file rests within the files in the root directory and can only be acquired after gaining privileges in the system.

7. **Web application**: Among the services in the vulnerable machine, a web server is on sight hiding 3 flags of the event. One will rest withing the source code of the home page and the other one is located in a hidden path that can't be accessed directly from the web page. It's intended to map the pages among the server to locate the hidden path and submit the last flag.

8. **Trivia:** Within this section, players will find trivia questions about protocols, history of hacking, networking, blockchain, OSI layers, among others.

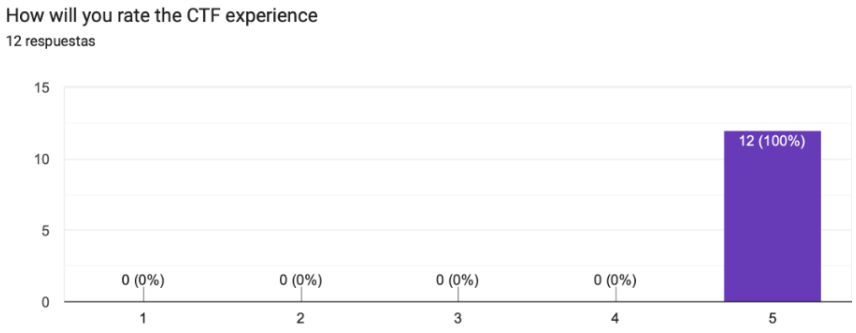
9. **Scoring Server**: This is intended to be hosted in AWS, it's already configured to register, without the necessity to validate or confirm, this will allow the tracking of the player's performance and the overall scoring chart. The challenges will have a total of 285 points divided as:

Name	Domain	Value
Warming Up	Cryptography	10
Decod3	Cryptography	10
Two56	Cryptography	10
Knocking the door	Reconnaissance	5
Sauron's Tranfer	Reconnaissance	5
Evil Server's IP	Reconnaissance	5
Evil Server's Users	Reconnaissance	5
Open Ports	Reconnaissance	10
Is it what you see?	Forensics	10
St3g	Forensics	10
St3g2	Forensics	10
Grep	Forensics	5
Evil's Network	Network Security	10
FTP 1	Network Security	5
FTP 2	Network Security	10
HTTP1	Network Security	5
The user agent	Network Security	5
E-Tag 1	Network Security	5
E-Tag 2	Network Security	5
Relat3d IP's	Network Security	10
Pr0tocols	Network Security	10
R00t	Privilege Escalation	20
Crawlers	Web Application	10
	Web Application	10
The Final Chapter	Web Application	10
The Final Chapter2	Web Application	20
Father of Father's	Trivia	5
Owasp T1-0	Trivia	5
1999	Trivia	5
Phishin	Trivia	5
PoW	Trivia	5
The Mask	Trivia	5
OSI	Trivia	5
Trickin	Trivia	5
It's Alive	Trivia	15
Survey	Survey	5

Chapter 5

Evaluation

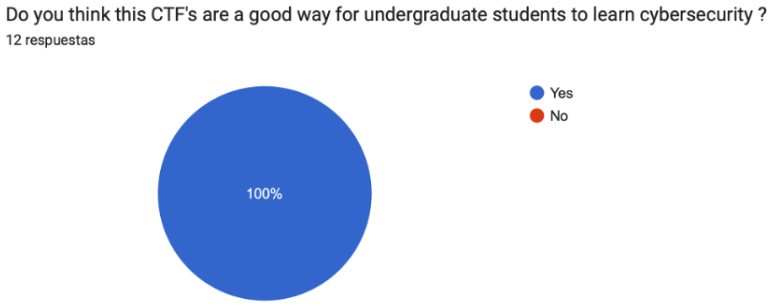
The described project was deployed using the hybrid version and 12 students from the Master of Science in Cybersecurity graduate program participated. This was lectured during the Spring term of 2024 at Sacred Heart University in Fairfield Connecticut. At the end of the exercise we provided a survey to the students to assess both sides of the scenario, trying to understand whether it was a good approach to improving skills by performing engaging scenarios or the setup needed extensive changes. While analyzing it to understand and identify if this is an effective way to help professors teaching Cybersecurity skills in an undergraduate environment we managed to identify a few points to deliver a better experience through the CTF, as well as specific points where the students identified as relevant and positive towards improving their skills. They are detailed below:



All of them voted the experience as an excellent scenario, engaging and fun.

All of them agreed that the CTF experience helped them to either assess or improve

their skills in the cybersecurity domain.



The majority of students agreed that these kinds of scenarios are a good way to teach students and improve their skills through hands-on experience.

In considering features that they think can be improved upon towards a better experience in the event, we asked the students: "What did you dislike about the overall experience?" and 6 out of the 12 students suggested that we make the flags non case sensitive allowing a more fluent experience as the answer they were providing was correct but the scoring server would not accept the answer because of a capital letter. Some students suggested using better phrasing to better assist in guiding them to their goals. The other suggestions for the CTF were to provide more free hints and make the challenges so that more software could be utilized.

Chapter 6

Conclusion

Several STEM curriculum's are aiming for the usage of blended models using traditional teaching schemes with immersive and engaging hands-on labs. This lends itself to enhancing the teaching and producing visible and successful implementation, as they are not only effective in students outcomes regarding these disciplines but also redefining the modern way to teach and help students understand core domains. This approach is not exclusive to cybersecurity. This approach could be potentially helpful in science, technology, engineering, and mathematics as well. In this paper we present a design of a CTF-based environment with a "Story telling" style. There are hints and manuals that will aid the students to acquire or enhance their skills within the core domains. These include cryptography, network security, web application security, digital forensics, privilege escalation, reconnaissance and usage of world-renowned tools. There are also the use of different operating systems such as Linux & Kali, and the command line interface to improve their problem-solving, analytical, teamwork, critical-thinking and attention to detail abilities. All the resources described in this paper will be available to the world through the following link: `https://drive.google.com/drive/folders/1AULkkW7kqRhNifBU6y8CPrsMU8aS1FVr?usp=sharing`

Bibliography

[1] J. Feiman, "Can stem qualifications hold the key to the future of cybersecurity?" 2019.

[2] "Market research report," 2023, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

[3] "Stem education strategic plan 2018," 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf.

[4] E.-C. C. Jay Vykopal, Valdemar Svabensky, "Benefits and pitfalls of using capture the flag games in university courses," 2020, https://arvix.org/pdf/2004.11556.pdf.

[5] M. Carlisle, M. Chiaramonte, and D. Caswell, "Using {CTFs} for an undergraduate cyber education," in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, 2015.

[6] M. Ellis, L. Baum, K. Filer, and S. H. Edwards, "Experience report: Exploring the use of ctf-based co-curricular instruction to increase student comfort and success in computing," in *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*, 2021, pp. 303–309.

[7] A. A. Giovanni Lagorio, Marina Ribaudo, "Capture the flag competition for higher education," 2021, https://ceur-ws.org/Vol-2940/paper38.pdf.

[8] https://aws.amazon.com.

[9] "Get started with the aws free tier," https://docs.aws.amazon.com/whitepapers/latest/how-aws-pricing-works/get-started-with-the-aws-free-tier.html.

[10] "Amazon ec2 on-demand pricing," https://aws.amazon.com/ec2/pricing/on-demand/.

[11] "How to import and export ova files in virtualbox," https://www.maketecheasier.com/import-export-ova-files-in-virtualbox/.

[12] "Deploy a virtual machine from an ovf or ova file in the vmware host client," https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.html.hostclient.doc/GUID-8ABDB2E1-DDBF-40E3-8ED6-DC857783E3E3.html.

[13] "Working with concurrency scaling," https://docs.aws.amazon.com/redshift/latest/dg/concurren
scaling.html.

[14] "Penetration testing phases: A roadmap to secure enterprise applications," https://successive.cloud/penetration-testing-phases/.