EDUCATION OF CYBER SECURITY AND INFORMATION SECURITY

Fernando Padilha Farah[1]; Everson Denis[2]

[1] Scholarship Student of the GCSP - IMT (EEM/CEUN-IMT)
[2] Mentor of the GCSP-IMT (EEM/CEUN-IMT

Article history: Received on 2021-12-03 / Presented at GCSP-IMT Seminar on 2021-12-09 /Available online from 2022-03-20

Abstract. *Nowadays there is a great shortfall of Cyber Security and Information Security experts, so every day there is a desperate need to teach and form professionals. A great way to do so is using a technic that involves active learning and gamification, such as CTF (or Capture The Flag). This Technic is based on quest and rewards, so every time the student receives a flag (normally a code string), they can retrieve it to receive a reward (commonly a punctuation to compete with others). This article presents the importance of cybersecurity and information security awareness, the skills acquired during the year 2021, as well as the use of the capture the flag (CTF) technique to demonstrate some domains of knowledge in the cybersecurity area.*

Keywords. *Cyber Security, Information Security, Education, Capture The Flag, Competencies.*

Introduction

Information security is directly related to the protection of a set of information, in the sense of preserving the value they have for an individual or an organization. The basic properties of information security are: confidentiality, integrity, availability, authenticity and non-repudiation.

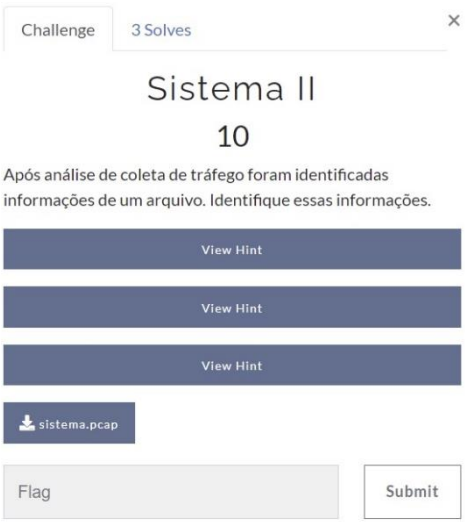
Cybersecurity is the practice of protecting critical systems and confidential information from potential cyberattacks. This practice has measures to combat threats against network systems and applications, regardless of whether that threat comes from within or outside the enterprise. Cyber awareness, when considered in the development and application of these new technologies, can at the same time deliver an innovation and drive even higher security levels and standards than previous technologies. Digital transformation and the increase in cybersecurity processes are elements that must go hand in hand. (WEF, 2021) revealed that cybersecurity flaws were indicated as the fourth biggest risk for the short term and that private and government actors are likely to engage in more dangerous and sophisticated cyberattacks in the near future. Therefore, it is essential that organizations look to the future in a pragmatic way, understanding the importance of having secure processes that follow the evolution of the technologies used.

In this context, we can prepare students and future professionals to raise awareness in the areas of Information Security and Cybersecurity using learning strategies, interactive platforms, extracurricular activities, academic competitions, among others.

CTF (Capture The Flag), is an active learning technique using questions to make participants acquire skills based on knowledge domains, such as Linux commands, forensics, cryptography, web exploration, among others. Quizzes were created with levels of difficulty, to develop technical skills, and the answer to these challenges provides the

score for each participant or for the team that is participating in the competition. Quizzes can present hints, add files for analysis, as well as the participants who solved them, partial and overall scores, as shown in Figure 1.

Figure 1 – CTF challenge - domain forensics (CTFD, 2021), (MAUACTF, 2021).



Objectives

The GCSP project (GCSP, 2021) during the year 2021 required some steps to be taken to acquire the necessary skills for the development of the platform and creation of the challenges in the CTF.

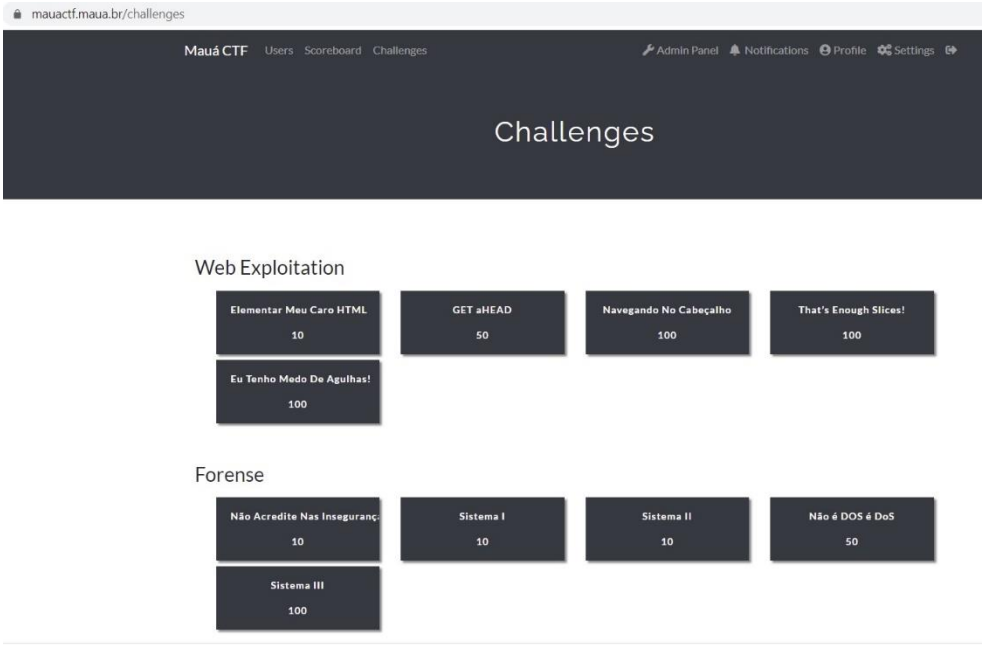
There was a suggestion from the mentor of the GCSP project, for the mentee to acquire the necessary technical skills to develop the project and assist in the preparation of the CTF, he should participate in the following PAEs activities (Projects and Special Activities): “CM2006 - LINUX ESSENTIALS” (NETACAD, 2021), "CM2011 - CYBERSECURITY" (MAUACTF, 2021), "CM2072 - PREPARATION FOR CYBER SECURITY CHALLENGES" (OPENLMS,2021), "CM4002 - CYBERSECURITY - CISCO NETWORKING ACADEMY" (OPENLMS,2021) (NETACAD, 2021) and "CM4042 - CLOUD COMPUTING - AWS ACADEMY” (AWS, 2021). The knowledge acquired in these PAEs was important for the development of the project and creation of the questions for the challenges in the CTFs, in addition to preparing for the Technical, Creative and Multidisciplinary competences.

Development

The first objective would be to understand the technical skills normally taught in these competitions. Thus, participating in competitions such as PicoCTF (PICOCTF, 2021), OverTheWire (OVERTHEWIRE, 2021), were interesting options to develop challenges based on multidisciplinary domains (operating systems, forensic analysis tools, web exploration, encryption, etc.). Platforms for creating CTF environments were also tested, after some research, the best platforms to be used were listed, such as CTFd

(CTFD, 2021) and FBCTF (FBCTF, 2021). The CTFd platform was chosen, due to the flexibility of configurations and available resources. In this context, the MauaCTF environment emerged (MAUACTF, 2021), as shown in Figure 2.

Figure 2: MauaCTF environment.

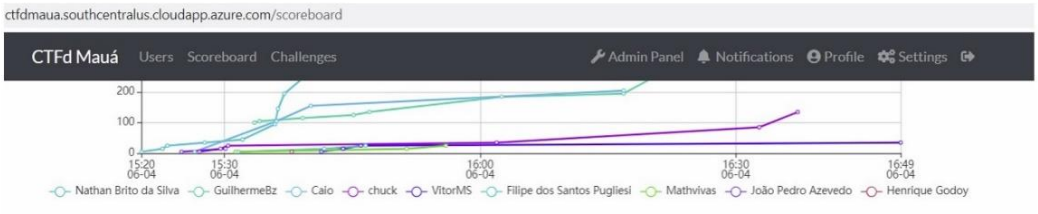


Before development, it was necessary to acquire necessary knowledge of operating systems (Linux and Windows), information security and cybersecurity, cloud environments to host the solution, in this way, the student participated in the following PAEs in 2021: “CM2006 - LINUX ESSENTIALS ”, “CM4002 - CYBER SECURITY - CISCO NETWORKING ACADEMY”, “CM2011 – CYBERSECURITY”, “CM2072 - PREPARATION FOR CYBER SECURITY CHALLENGES” and “CM4042 - CLOUD COMPUTING - AWS ACADEMY”.

To test the CTFd environment, the first test was performed in virtual machine environments using a virtualized instance of the Ubuntu Linux operating system running on a real machine with Windows 10, where it was possible to measure the real resources needed. for the preparation of a real system to be later hosted on servers in its own datacenter or in the cloud. As the student already had initial skills with the Azure cloud environment, the MauaCTF environment tests were tested in the Azure environment (AZURE, 2021).

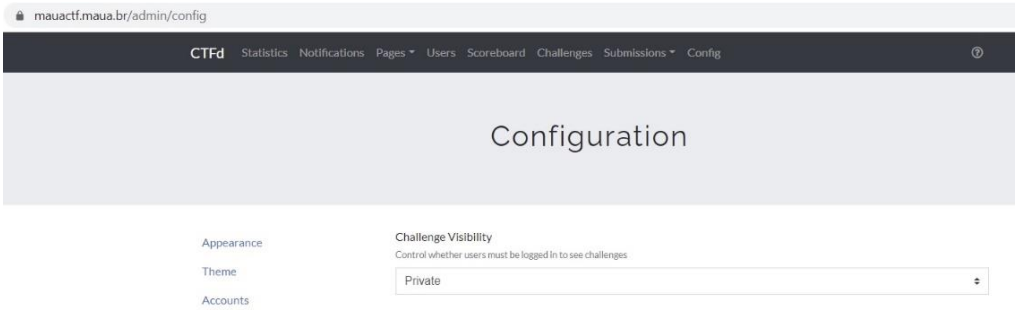
The MauaCTF platform was offered to the internal and external public in 2 moments: At the end of the PAE “CM2072 - PREPARATION FOR CYBER SECURITY CHALLENGES” at the end of the 1st semester of 2021 using the Azure cloud environment, only for Maua students, as shown in Figure 3.

Figure 3: MauaCTF hosted on Azure.



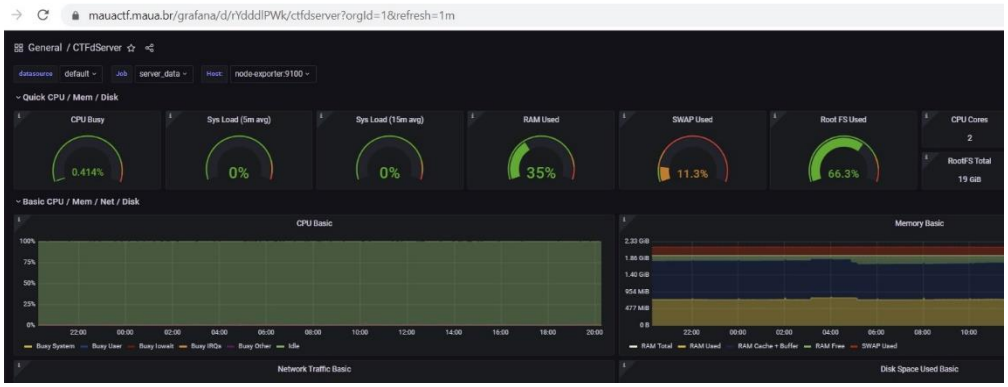
Considering the necessary requirements of virtual machines using in the Azure cloud environment, the MauaCTF environment was hosted in the Mauá Datacenter. At the end of the 2nd semester, new challenges were offered both for Maua students and for the external public (students from other institutions and professionals in the information security area), as shown in Figure 4.

Figure 4: MauaCTF hosted in Datacenter on-premises.



During the development to implement the solution in the Mauá Datacenter, an SSL/TLS certificate solution was implemented to protect data traffic between client and WEB server from some common attacks and exploits (NPM, 2021). Some services were configured, such as Prometheus (PROMETHEUS, 2021) and Grafana (GRAFANA, 2021) to monitor the system, such as CPU usage, network, RAM usage, among others, in addition to displaying customizable dashboards and graphics via the WEB (figure 5).

Figure 5: Monitoring - MauaCTF hosted in Datacenter on-premises.



Results and Discussion

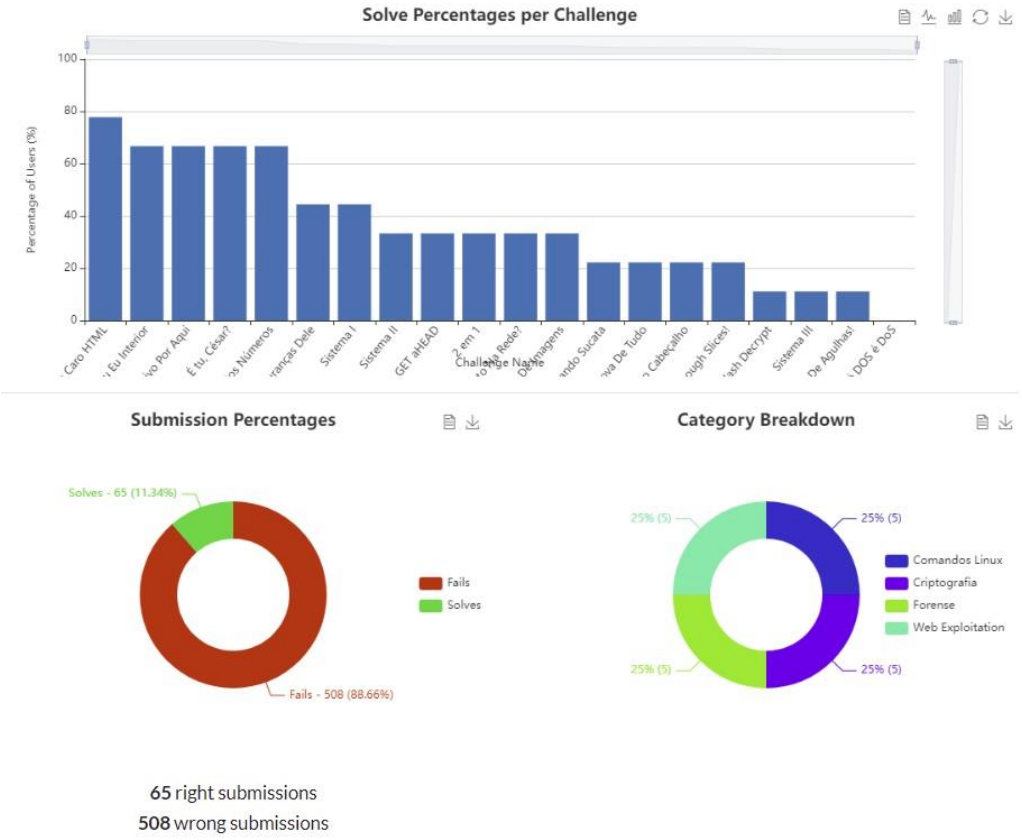
At the end of the 2nd semester, new challenges were offered both to Mauá students and to the external public (students from other institutions and professionals in the information security area). There were 7 days of different challenges divided into 4 domains of knowledge (Linux commands, forensics, encryption and web exploration) with different levels of difficulty (10, 50 and 100), allowing participants a competitive environment between them (figure 6).

Figure 6: Challenges - MauaCTF hosted in Datacenter on-premises.

Conecte-se Com Seu Eu Interior	Comandos Linux	10
Eu Sei Que Deixei O Arquivo Por Aqui	Comandos Linux	10
Vasculhando Sucata	Comandos Linux	50
Não é DOS é DoS	Forense	50
Não Acredite Nas Inseguranças Dele	Forense	10
Elementar Meu Caro HTML	Web Exploitation	10
GET aHEAD	Web Exploitation	50
É tu, César?	Criptografia	10
Arte Dos Números	Criptografia	50
Pode Fazer Gato Na Rede?	Comandos Linux	100
Eu Sou Aprova De Tudo	Comandos Linux	100
Navegando No Cabeçalho	Web Exploitation	100
Sanduíche De Imagens	Criptografia	100
Hash Decrypt	Criptografia	100
2 em 1	Criptografia	50
Sistema I	Forense	10
Sistema II	Forense	10
Sistema III	Forense	100
That's Enough Slices!	Web Exploitation	100
Eu Tenho Medo De Agulhas!	Web Exploitation	100

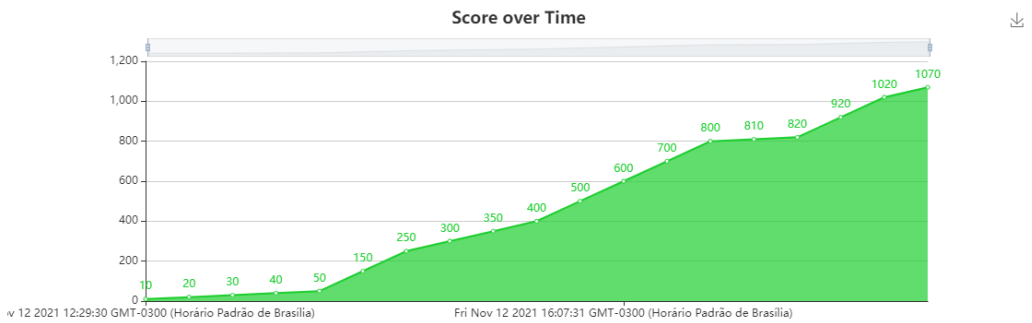
Although the participants had a lot of difficulty, especially in the first half of the competition, there were many occasions when they sought guidance. This proved how engaging and inspiring CTF competition can be (figure 7).

Figure 7: Participant's score over time.



As shown in Figure 8, several topics from the 4 domains were discussed, thus, throughout the competition, participants added new knowledge and developed new skills providing active learning.

Figure 8 - Score over time of a particular participant.



Conclusion

Since the beginning of the GCSP project (GCSP, 2021), many skills were created and developed throughout 2021 for the mentored student Fernando Padilha Farah. Technical, creative and multidisciplinary skills were developed during the participation of PAEs and development of the CTF environment, in addition to the preparation of quizzes. Multicultural and empathetic skills were developed in an action by the student Fernando as president of a group of students focused on making the college a more diverse place, discussing topics that were not widely known. Multidisciplinary and social awareness skills were worked on at GCSP events, such as the North Dakota Congress and the GCSP Network Annual Meeting, where it was possible to debate the themes and have a broader view of the challenges in the context of the GCSP, mainly to discuss the topic. with people from different backgrounds and ideas, with new ways of looking at the aspects involved in Cyber Security.

In the elaboration of the CTF environment (CTFD, 2021), (MAUACTF, 2021), active learning concepts were worked on, such as gamification, which proved to be quite effective in engaging students and professionals in the cybersecurity area with real problems (MACDANIEL and TALVI, 2016), (FORD and SIRAJ, 2017), (KUCEK and LEITNER, 2019).

References

AWS, AWS Academy. Available in: https://www.awsacademy.com/LMS_Login. Access in: 02 dec. 2021.

AZURE. Build in the cloud free with Azure for Students. Available in: https://azureforeducation.microsoft.com. Access in: 02 dec. 2021.

CTFD, Cyber Security Training made simple. Available in: https://ctfd.io. Access in: 02 dec. 2021.

FBCTF, The Facebook CTF is a platform to host Jeopardy and “King of the Hill” style Capture the Flag competitions. Available in: https://github.com/facebookarchive/fbctf. Access in: 02 dec. 2021.

FORD, Vitaly; SIRAJ, Ambareen Capture the Flag Unplugged: An Offline Cyber Competition, ACM Digital Library, 2017.

GCSP, Grand Challenges Scholars Program. Available in: http://www.engineeringchallenges.org/challenges/cyberspace.aspx. Access in: 02 dec. 2021.

GRAFANA, Operational dashboards for your data here, there or anywhere. Available in: https://grafana.com. Access in: 02 dec. 2021.

KUCEK, Stela; LEITNER, Maria. An Empirical survey of functions and configurations of open-source capture the Flag (CTF) environments, Journal of Network and Computer Applications, 2019

MACDANIEL, Lucas; TALVI, Erik, Capture the Flag as Cyber Security Introduction, 49th Hawaii International Conference on System Sciences, 2016.

MAUACTF, Capture the Flag - Instituto Mauá de Tecnologia. Available in: https://mauactf.maua.br. Access in: 02 dec. 2021.

NETACAD. Cisco Networking Academy, Empowering everyone with career possibilities. Available in: https://www.netacad.com/pt-br. Access in: 02 dec. 2021.

NPM. Nginx Proxy Manager: Expose your services easily and securely. Available in: https://nginxproxymanager.com. Access in: 02 dec. 2021.

OVERTHEWIRE, Wargames. Available in: https://overthewire.org/wargames. Access in: 02 dec. 2021.

OPENLMS, Why use Open LMS? Because Open LMS is the best and easiest solution for teaching and learning. Available in: https://imt.myopenlms.net. Access in: 02 dec. 2021.

PICOCTF, Carnegie Mellon University. Available in: https://picoctf.org. Access in: 02 dec. 2021.

PROMETEUS, Power your metrics and alerting with the leading open-source monitoring solution. Available in: https://prometheus.io. Access in: 02 dec. 2021.

WEF. World Economic Forum: The Global Risks Report 2021. Available in: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf. Access in: 02 dec. 2021.