Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.152-168, 2023.
DOI: 10.18762/1982-4920.20230010

O USO DE CAPTURE THE FLAG PARA O APRENDIZADO E APERFEICOAMENTO EM SEGURANCA DA INFORMAÇÃO

Yara Franciele Parra, Wdson de Oliveira

RESUMO

A segurança da informação está em constante evolução e exige uma abordagem multidimensional para proteger as informações e mitigar os riscos cibernéticos. No ano de 2021, várias empresas enfrentaram ataques cibernéticos devido à falta de proteção de dados, o que levou à criação da Lei Geral de Proteção de Dados Pessoais (LGPD) para auxiliar na proteção dos dados. No entanto, as empresas precisam se adequar às propostas da LGPD e promover uma cultura de segurança. Uma forma de treinar e desenvolver habilidades em segurança da informação é por meio do Capture The Flag (CTF), uma competição gamificada relacionada à segurança da informação. O CTF oferece diferentes modalidades, como *Jeopardy*, competições em grupo e boot2root, que permitem aos participantes solucionar desafios relacionados a criptografia, programação, redes e *pentest.*Este artigo tem como objetivo apresentar como a implementação do Capture The Flag pode beneficiar as empresas na garantia da segurança da informação. Serão mostradas duas interfaces de sites que oferecem plataformas de CTF.

Palavras-chave: Capture the flag, segurança, informação, CTF.

ABSTRACT

Information security is constantly evolving and requires a multidimensional approach to protect information and mitigate cyber risks. In 2021, various companies faced cyber attacks due to inadequate data protection, leading to the enactment of the General Data Protection Law (LGPD) to support data protection efforts. However, organizations still need to align with LGPD proposals and foster a culture of security.One way to train and develop skills in information security is through Capture The Flag (CTF), a gamified competition related to information security. CTF offers different modalities, such as Jeopardy, group competitions, and boot2root, allowing participants to solve challenges in areas like cryptography, programming, networks, and penetration testing.This article aims to demonstrate how the implementation of Capture The Flag can benefit companies in ensuring information security. Two website interfaces with CTF platforms will be presented.

Keywords: Capture the flag, security, information, CTF

1. INTRODUÇÃO

A Segurança da informação esta em constante evolução, que exige uma abordagem multidimensional para proteger as informações e mitigar os riscos

cibernéticos. As organizações devem investir em tecnologias avançadas, implementar boas práticas de segurança, manter-se atualizadas com as regulamentações aplicáveis e promover uma cultura de segurança em todos os níveis da organização.

Com base na informação anterior e de acordo com consultoria Accenture publicado pela Folha de São Paulo em 22 de fevereiro de 2022 no site do uol, o ano de 2021 foi de muita agitação na área da tecnologia para diferentes empresas que não tinham proteção de dados, ano com uma grande ocorrência de ataques de cracker, nos quais as organizações tiveram suas informações nas mãos de bandidos, correndo risco de serem expostas.

Esse grande volume de ataques impulsionou o governo a sancionar uma lei conhecida como a Lei Geral de Proteção de Dados Pessoa (LGPD) criada em 2014 e sancionada somente em 2018, sendo exigida somente em 2021, no qual o objetivo é apoiar as empresas no quesito proteção de dados. Mesmo que ratificada, ainda não estava garantindo a segurança total da empresa, considerando que ainda seriam necessárias as organizações se adequarem as propostas da LGPD, para garantirem a segurança da informação, adquirindo métodos de treinamentos, e fornecê-los aos seus colaboradores, para que houvesse um trabalho em conjunto a fim de garantir a segurança e proteção da empresa e de seus bens.

Baseado nesse contexto, várias empresas de tecnologia criaram sites onde fosse possível treinar habilidades para detectar vulnerabilidades e falhas em sistemas e consequentemente, uma forma de como proteger os sistemas de ataques por pessoas mal-intencionadas.

Com o propósito de treinar o conhecimento das pessoas, existe o Capture The Flag (CTF), que é uma modalidade de competição gameficada, diretamente relacionado a segurança da informação, onde o indivíduo é desafiado a solucionar problemas proposto pela aplicação utilizada. É importante ressaltar que existe um determinado tempo para os desafios serem resolvidos. Diversos temas são encontrados para serem utilizados em seus estudos, sendo os mais famosos: criptografia, programação, redes, *pentest* entre outros.

Existem várias formas de praticar o CTF, dentre elas, encontramos o *Jeopardy*. Nesta modalidade é apresentado vários desafios e o usuário precisa desvendar as barreiras propostas para conseguir quebrar as vulnerabilidades, outra modalidade é a de realizar a jogatina em grupo, onde cada grupo recebe um desafio e tem que proteger suas vulnerabilidades e tentar quebrar as do adversário, com isso, quem

proteger e quebrar as fraquezas do outro sai como campeão da partida, e para aquele que não quer praticar nenhuma das duas modalidades citadas anteriormente, existe também a *boot2roo*t, onde o jogador pratica contra um computador, seu objetivo é invadir o software utilizando permissão de acesso.

De acordo com o contexto apresentado, este artigo tem como objetivo mostrar como o uso do *Capture the Flag* será benéfico para as empresas implementarem ele em suas organizando, com o intuito de garantir a segurança da informação delas, com isso será apresentado interface de dois sites que tem uma plataforma de *Capture the Flag.*

2. REFERENCIAL TEÓRICO

Serão apresentadas, a seguir, os principais conceitos para fundamentar o tema do projeto em questão. O referencial teórico foi escrito a partir da leitura de vários documentos de autores que escreveram sobre o assunto, tais como Quintella e Branco, Peixoto, Magalhaes, Cohen Chung, Mena, Gonzales, Seltzer e Mansurov.

2.1 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada (FONTES, 2006, n.p.).

Desde seus primórdios a espécie humana acumula informações, seja através da fala ou forma física, demonstrando o grande valor para sua evolução e crescimento. Portanto, a segurança torna-se um ativo de grande importância e que deve ser protegido.

Em meio a um cenário de rápido desenvolvimento e compartilhamento de informações, o universo dos conteúdos digitais está sujeito a várias ameaças que podem comprometer a segurança da informação dos seus usuários (SOTO, 2022).

Segundo Quintella e Branco (2013, p. 2), Segurança da Informação diz respeito à “proteção da informação contra ameaças que possam valer-se das vulnerabilidades dos ativos, preservando suas propriedades fundamentais: disponibilidade, integridade e confidencialidade”.

Bem como, é importante ressaltar que, atualmente, a maioria das informações das empresas estão armazenadas em meios digitais, o que aumenta a importância da segurança da informação em relação à proteção de dados eletrônicos. Ademais, as informações podem assumir diferentes formatos, desde arquivos de texto até bancos de dados complexos, e cada formato exige abordagens específicas de segurança para proteger as informações de acordo com as suas características e níveis de risco.

Segundo Peixoto (2006), a Segurança da Informação é formada pelos seguintes pilares básicos, que podem ser definidos da seguinte maneira.

- Disponibilidade (*Availability*): Para que quaisquer informações atendam ao seu propósito, elas devem estar disponíveis quando necessário.
- Confidencialidade (C*onfidentiality*): Na segurança da informação, confidencialidade tem o objetivo de garantir que determinada informação não seja disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados. Por exemplo seus dados eletrônicos como senhas ou números de cartões de crédito.
- Integridade *(Integrity*): A integridade dos dados significa manter e assegurar a precisão da informação durante todo o seu ciclo de vida. Isso significa que os dados não podem ser modificados de maneira não autorizada ou não detectada. (EUNERD, 2021)

2.2 Conceito de *Capture The Flag*

No âmbito da tecnologia da informação, competições de CTF envolvem diferentes habilidades dos jogadores para resolução de desafios de segurança da informação. Segundo [Magalhaes et al. 2017].

O CTF é um tipo de jogo ou competição em que os participantes tentam encontrar e explorar vulnerabilidades em sistemas de computador, enquanto protegem seus próprios sistemas de ataques dos adversários.

As competições são usadas pela comunidade de segurança de computadores para fins de educação e avaliação, sendo considerada uma excelente abordagem para aprender conceitos técnicos em ambiente de aprendizado (CHUNG; COHEN,2014).

Os jogadores geralmente são divididos em equipes, e cada equipe é encarregada de defender um sistema enquanto tenta invadir o sistema da equipe adversária para encontrar uma "bandeira" ou "objeto" escondido. A equipe que consegue capturar a bandeira do adversário e levá-la de volta à sua própria base é a

vencedora. As competições de CTFs são direcionadas aos profissionais da área de cibersegurança, nas quais formam-se equipes destinadas às competições realizadas em eventos regionais, nacionais e internacionais, em que geralmente são ofertadas como recompensas grandes dinheiro. Outros eventos são voltados para estudantes da área, e ocasionalmente existe um apoio financeiro para os competidores que se destacam durante o evento. Além disso, algumas empresas observam os participantes durante as competições com o intuito de selecionar os mesmos para fazerem parte do seu quadro de colaboradores. (Mena, 2018)

Os desafios em um CTF podem envolver tarefas como análise de código, exploração de vulnerabilidades, engenharia reversa, criptografia e outras habilidades técnicas relacionadas à segurança cibernética. CTFs são frequentemente usados para treinar e testar habilidades de segurança cibernética, e muitas vezes são realizados em eventos ao vivo ou online.

Entende-se que o CTF pode desenvolver as habilidades dos competidores a área de segurança, mas habilidades que eles já possuem também as que podem ser adquiridas através de estudos, prática em ambientes controlados (treinamentos) ou profissionalmente descrevendo uma ampla gama de técnicas como criptografia, redes, programação, *cloud computing*, *pentest, e*ngenharia reversa*,* exploração de binários análise forense e estenografia (GONZALES et al.,2019) .

2.3 Tipos de *Capture the Flag*

Segundo Seltzer(2019) e o site CTF Zone, as competições podem ocorrer em três modalidades, sendo que, cada uma delas podem ser realizadas de duas formas: individualmente ou em equipe, e seus estilos são *Jeopardy,* Ataque e defesa*, King of the hill e* linear.

2.3.1 Jeopardy

O estilo *Jeopardy* é baseado em quizzes (questionários) referentes à área de segurança da informação, com a finalidade de testar os conhecimentos dos competidores e ou estudantes em determinados assuntos da cibersegurança, quais sejam: a criptografia, redes, programação, *cloud computing*, *pentest, e*ngenharia reversa*,* exploração de binários análise forense e estenografia, em que os competidores dessa modalidade podem trabalhar sozinhos ou com uma equipe (RAJ et al., 2016).

Os jogos CTF no estilo de *Jeopardy* colocam os organizadores executando um conjunto de desafios que cada individuo ou equipe precisa resolver por pontos. Em geral, quanto mais complicada a tarefa, mais pontos são conquistados. Os desafios são geralmente independentes um dos outros e, idealmente, entre os jogadores conectados, o que leva à confiabilidade e estabilidade para grandes competições. A pontuação também é simples e agradável: some os pontos para os desafios resolvidos e use o tempo das soluções para desempatar (CAPTURE, 2019).

2.3.2 Ataque e defesa

O estilo Ataque e Defesa exige maior conhecimento e experiencia dos participantes, sendo necessário utilizar ferramentas de *hackers,* exportar e corrigir vulnerabilidades. Estabelece assim uma barreira para alunos iniciantes na área, pois os problemas simulados nesse tipo de competição equiparam-se à vida real, haja vista que exige um alto nível de conhecimento (MANSUROV, 2016).

As competições consistem na formulação de duas equipes. Cada uma das equipes possui um ambiente computacional preparado, salientando que esse tipo de competições pode ocorrer de forma online ou local. Nessa modalidade, uma equipe tenta realizar ataques ao sistema da outra e defender o seu próprio sistema. Nesse gênero específico de competição, as equipes de defesa podem preparar seus sistemas como desejarem, corrigindo todas as vulnerabilidades que forem perceptíveis e deixando somente os serviços necessários abertos no firewall. Em contrapartida, os atacantes podem utilizar técnicas de intrusão para obter privilégios e informações (SELTZER, 2019).

2.3.3 King of the Hil

King of the hill é um estilo de CTF que consiste em uma rede de computadores que contêm um servidor com um serviço vulnerável, em que os competidores devem manter o controle do maior número de serviços pelo maior tempo possível para pontuar. Esse estilo é caracterizado como um *pentest (*SELTZER, 2019).

O objetivo dos participantes do *King of the Hill* é detectar vulnerabilidades dos sistemas, explorá-las, e o mais importante de tudo, mantes o controle sobre os sistemas pelo maior tempo possível. O truque está na regeneração dos conjuntos de

vulnerabilidades nos sistemas. Os participantes enfrentam um dilema, tentar atacar os vizinhos ou prosseguir com a detecção de vulnerabilidades nos sistemas que já está sob controle [...] (PHDAYS, 2012, n.p., tradução nossa).

3 METODOLOGIA

Com o intuito de contextualizar o tema do artigo em questão foi desenvolvida uma pesquisa bibliográfica baseada em artigos, sites e livros procurando fazer um levantamento destacando pontos e contrapontos para melhor discernimento de como utilizar o *Capture The Flag,* seu uso para o aprendizado e aperfeiçoamento e como ele afeta as empresas e a partir desse ponto alcançar os objetivos propostos para no início do projeto de graduação.

A didática almejada na transcrição do estudo tem a propensão de mostrar de que forma essas ações podem colaborar para que as empresas comecem a utilizar o *Capture The Flag* visando garantir uma melhora e maior segurança dos dados e ativos de sua empresa.

Será feito uma apresentação do funcionamento da plataforma de *Capture the Flag* que a empresa Google disponibiliza, mostrando alguns desafios, com o intuito de despertar interesse pelas empresas em treinar seus colaboradores utilizando a ferramenta como defesa.

4 RESULTADOS E DISCUSSÃO

Para demonstrar o funcionamento do *Capture the flag* foi realizado *screenshot* de duas plataformas que disponibilizam para todos os usuários que utilizarem elas possam aprender e praticar CTF. O intuído de utilizar estas capturas de tela é para demonstrar o funcionamento na prática e que realmente funciona.

4.1 Plataforma CTFLEARN

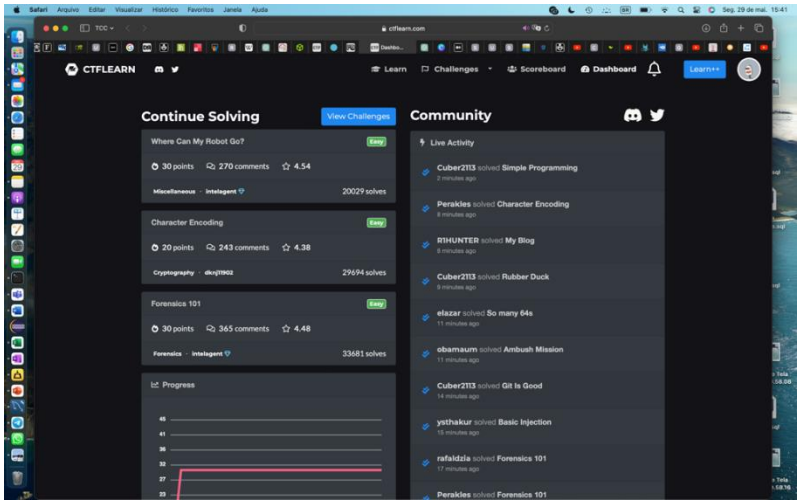
A Figura 1 apresenta a plataforma CTFLEARN ela é uma plataforma online que disponibiliza desafios voltados para segurança cibernética com formato de *Capture The Flag*, esta plataforma tem com intuito proporcionar um ambiente de aprendizado

pratico e desafiador. Contendo muitos desafios e que abrange várias categorias de segurança cibernética sendo eles criptografia, forense digital, exploração de software, *web hacking*, engenharia reversa, entre outras categorias existente.

A plataforma projeta desafios com o intuito de representar um cenário no mundo real, que os participantes poderão resolver os problemas, podendo também coletar informações e encontrar vulnerabilidades que serão de grane utilidade para alcançar os objetivos que estão sendo proposto.

A plataforma pode ser utilizada de forma gratuita ou se desejar mais recursos só assinar os pacotes que são oferecidos.

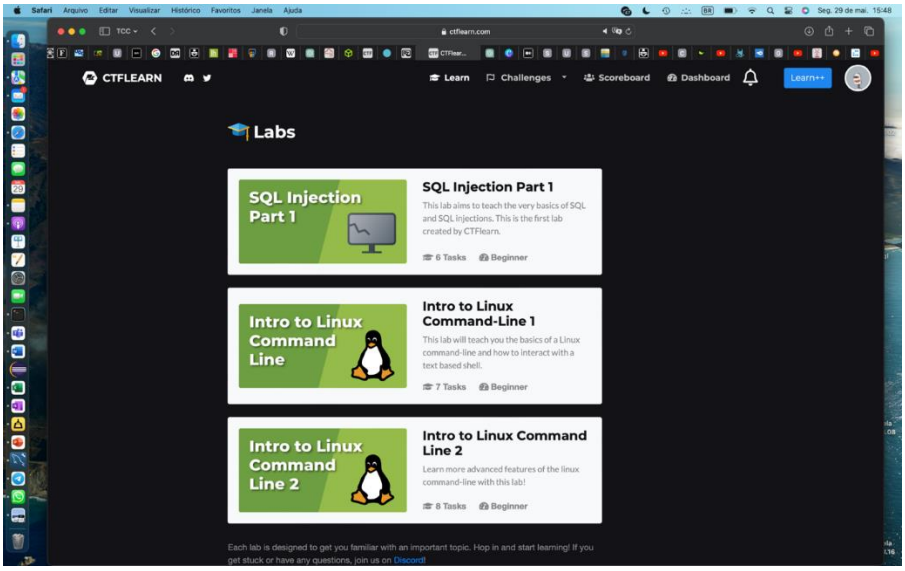
Figura 1- Site CTFLEARN



Fonte: *Screenshot* feita pelo autor

Na plataforma do CTFLEARN, conforme apresentado na Figura 2, é possível encontrar uma secção onde pode se obter acesso a matérias educacionais que a plataforma disponibiliza com intuito de ajudar os participantes a desenvolverem suas habilidades, nessas secções são disponibilizados tutoriais, artigos explicativos, guias com passo a passo, entre outros recursos que possam instruir quem estiver interessado em aprender mais.

Figura 2- Interface *labs* do site CTFLEARN



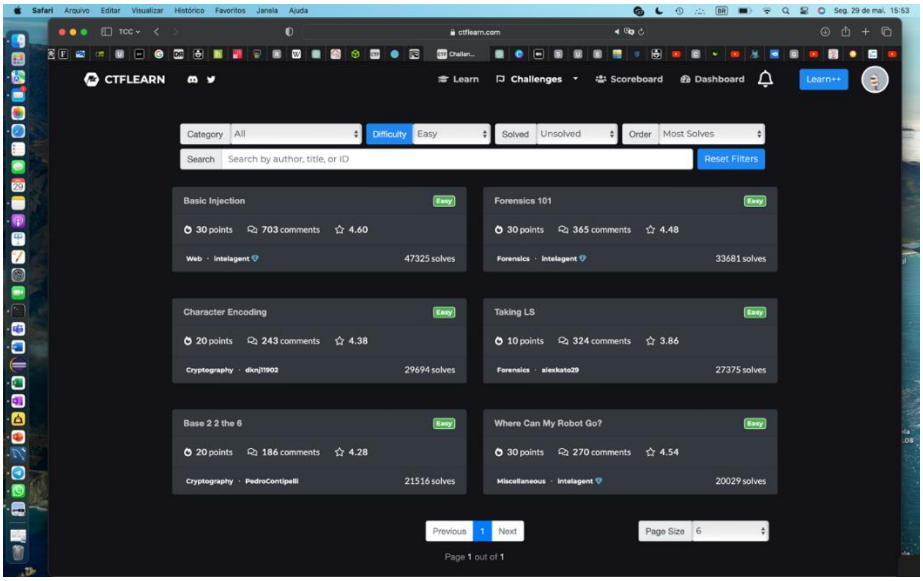
Fonte: *Screenshot* feita pelo autor

Sendo a parte mais importe da plataforma, a seção *challenges* é onde os participantes tem acesso a variedade de desafios de segurança cibernética que estão disponíveis para resolução, como dito anteriormente são desafios projetados para testar e aprimorar as habilidades dos participantes de diversas áreas, incluindo as que foram citadas.

Estes desafios são apresentados com o objetivo de encontrar uma solução para eles, ao resolvê-los os participantes adquirem conhecimentos práticos e também ganham experiência em aplicar técnicas de segurança cibernética no mundo real, para proteger as empresas de possíveis ataques.

De acordo com a Figura 3, os desafios podem variar desde as categorias até os níveis de dificuldades apresentada em cada desafio, possibilitando que os participantes possam adquirir diversas habilidades e encontrar qual sua principal necessidade.

Figura 3- Interface *challenges* do site CTFLEARN



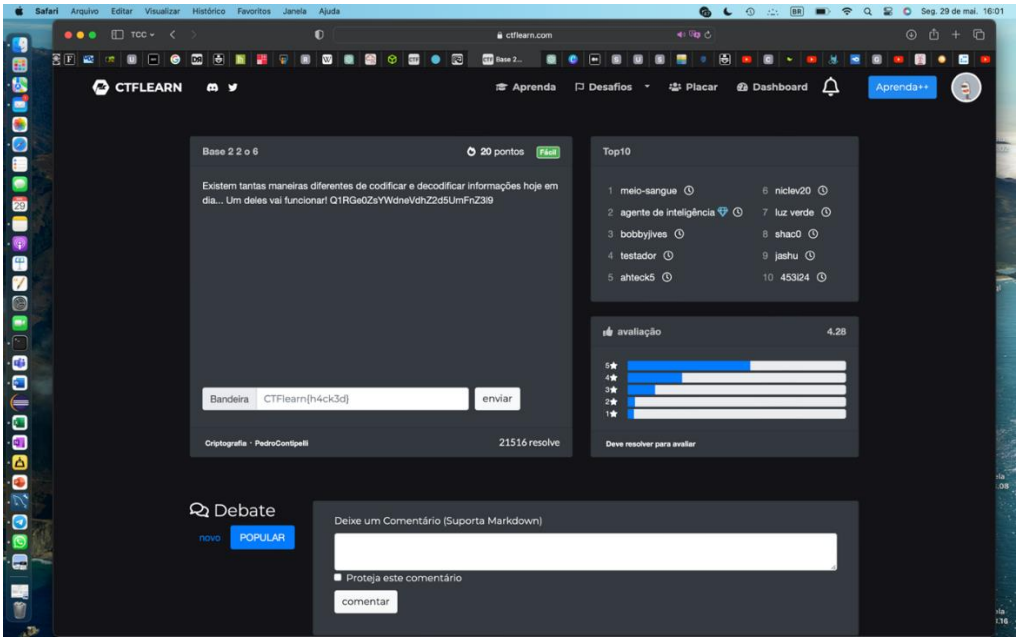
Fonte: Screenshot feita pelo autor

Na figura 4 é possível ver que a plataforma fornece a descrição do desafio, o contexto e as informações mais relevantes que podem auxiliar os participantes a solucionar este desafio. Varia de desafio para desafio, mas também é disponibilizado arquivo para analise, códigos para serem examinados, links de websites com vulnerabilidade, e muitos outros recursos.

Nesta tela também é possível ver a classificação deste desafio, e a pontuação do top10, tem também o espaço para comentários caso deseja realizar um ou então rolando a barra é possível verificar o comentário de outros membros desta comunidade que deixaram lá seus comentários.

Com base no que é solicitado neste desafio que é de criptografia fiz uma busca para encontrar um site que fizesse a descriptografia do texto embaralhado que o site deu neste desafio.

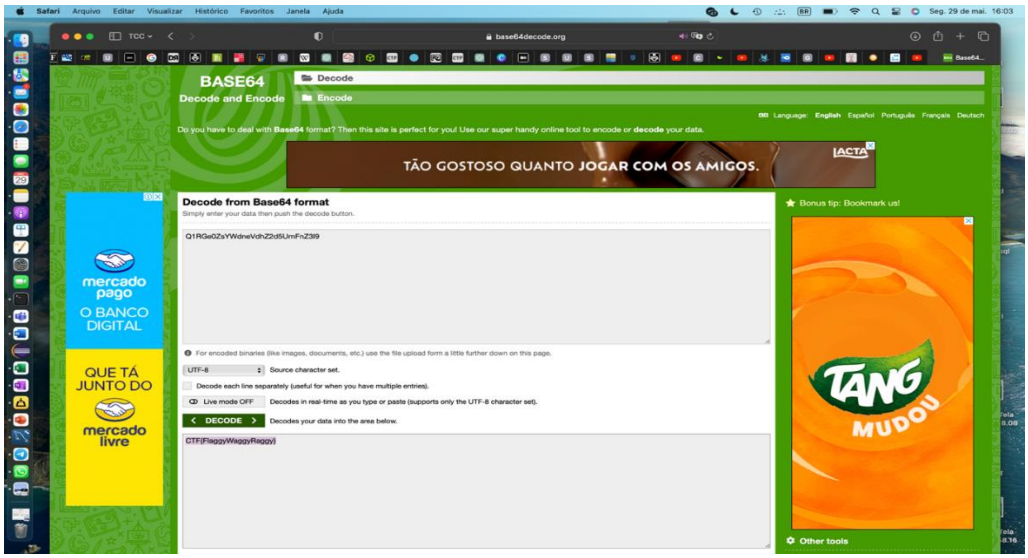
Figura 4- Interface do desafio do site CTFLEARN



Fonte: *Screenshot* feita pelo autor

No site escolhido que esta sendo representado pela imagem 5, foi adicionado o texto disponibilizado pela plataforma CTFLEARN e então decodificado, ele retornou uma frase como mostra na imagem.

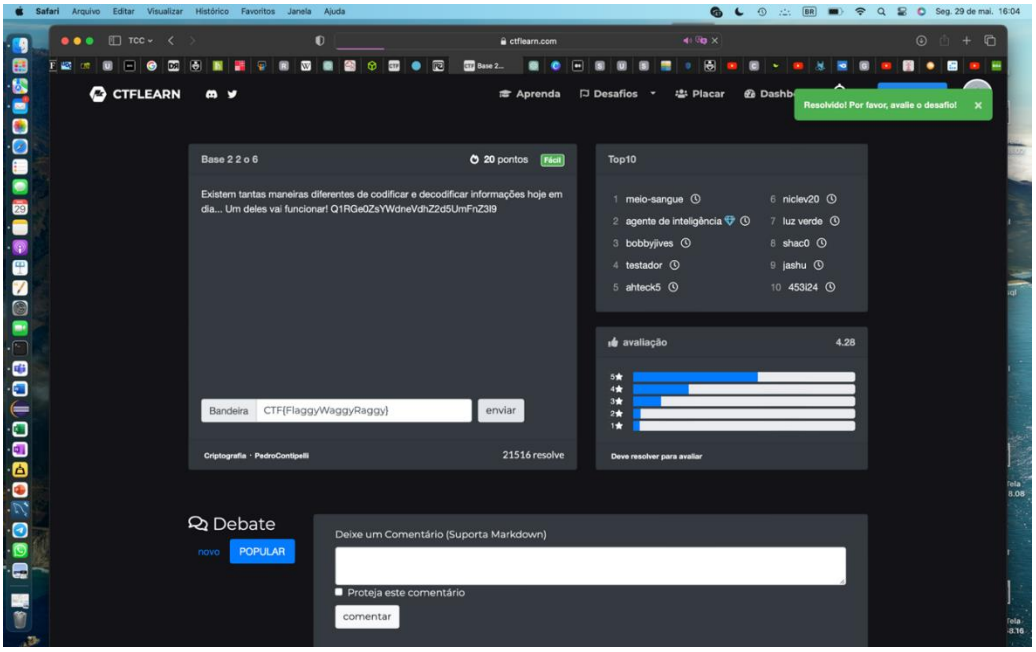
Figura 5- Interface do site de criptografia



Fonte: *Screenshot* feita pelo autor

Nesta imagem na parte da resposta coloquei o texto descriptografado e então submeti a resposta =, onde pude adquirir 20 pontos, pois a resposta era a que eles esperavam.

Figura 6- Interface do desafio do site CFTLEARN



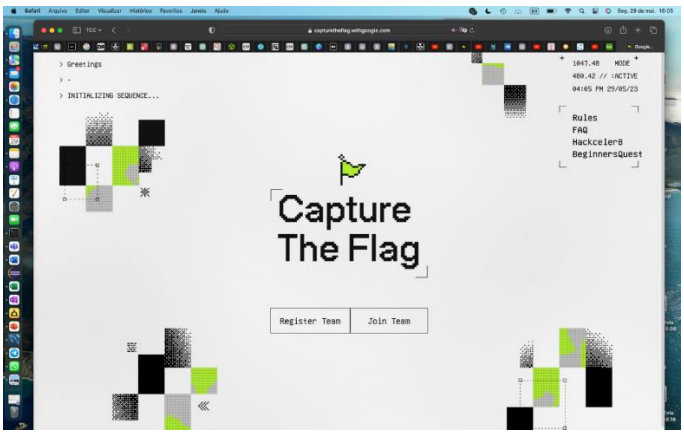
Fonte: *Screenshot* feita pelo autor

4.2 Plataforma GCTF

O Google tem sido um defensor ativo da segurança cibernética e tem participado de competições de CTF, tanto como organizador quanto como participante. O Google CTF, por exemplo, é um evento anual organizado pela empresa, onde os competidores enfrentam desafios de segurança cibernética em várias categorias.

Na figura 7 esta representado a página inicial da interface do google, e nela que é fornecida as informações gerais sobre o CTF, incluindo as regras, cronograma, categorias de desafios e pontuação atual.

Figura 7- Interface do GCTF



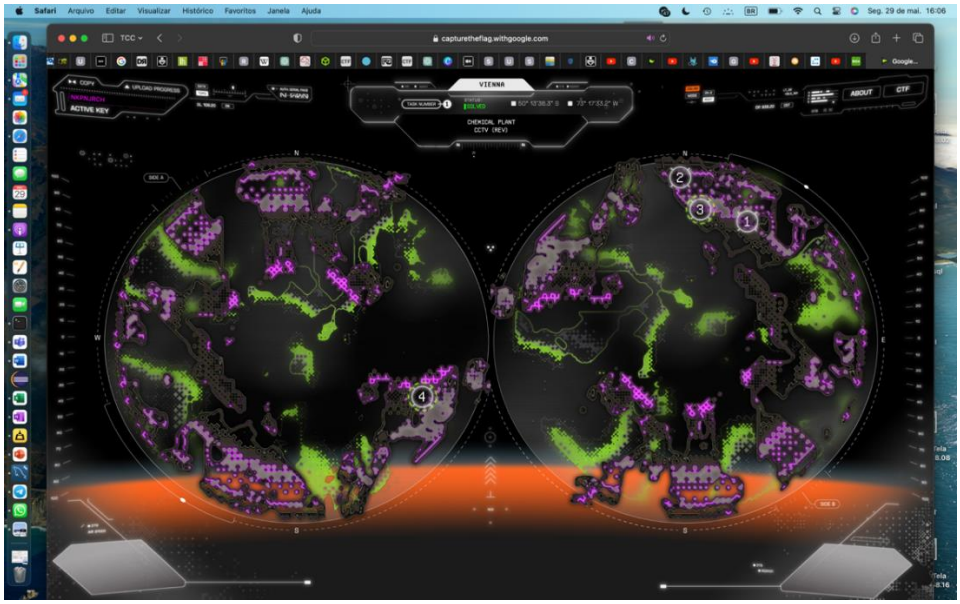
Fonte: *Screenshot* feita pelo autor

Nesta seção "*beginnersQuest*" que está sendo mostra na figura 8 ela é projetada para fornecer um conjunto de desafios mais acessíveis e amigáveis para participantes iniciantes em segurança cibernética e CTFs. Esses desafios são cuidadosamente desenvolvidos para ajudar os iniciantes a aprender os conceitos básicos, ganhar experiência prática e construir uma base sólida para enfrentar desafios mais avançados.

O principal objetivo desta seção que está sendo representa na Figura 8 é proporcionar uma experiencia de aprendizado gradual, onde os participantes possam adquirir confiança, aprender técnicas fundamentais e obter uma compreensão básica dos princípios de segurança cibernética. É uma oportunidade para os iniciantes praticarem suas habilidades, ganharem exposição a diferentes áreas da segurança cibernética.

Como pode-se observar nesta tela tem duas circunferências, inicialmente ela vem somente com o número 1 que é o primeiro desafio a ser solucionado, ao clicar nele irá abrir outra guia

Figura 8 – Interface do "*BeginnerQuest*" do GCTF



Fonte: Screenshot feita pelo autor

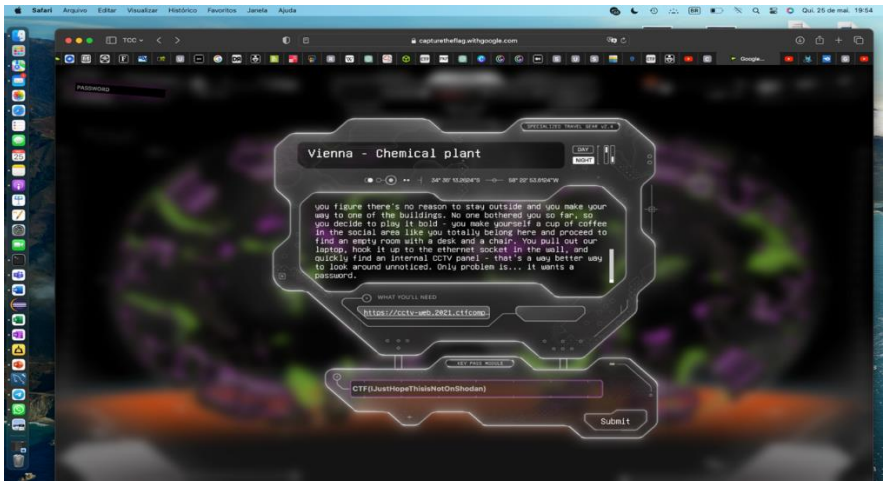
Ao abrir o item 1 para resolver o problema ele me leva até esta página representa na figura 9 que é onde estão as instruções para solucionar o primeiro desafio, ela vem acompanhada de um link, ao clicar nele você será redirecionado a

outra página.

Neste ponto é importante tentar obter o máximo de informações possível para facilitar a desvendar o desafio, e então solucioná-lo.

Nesta tela tem um link que será utilizado para descobrir a chave e liberar o acesso as câmeras que será útil para ir para a próxima fase.

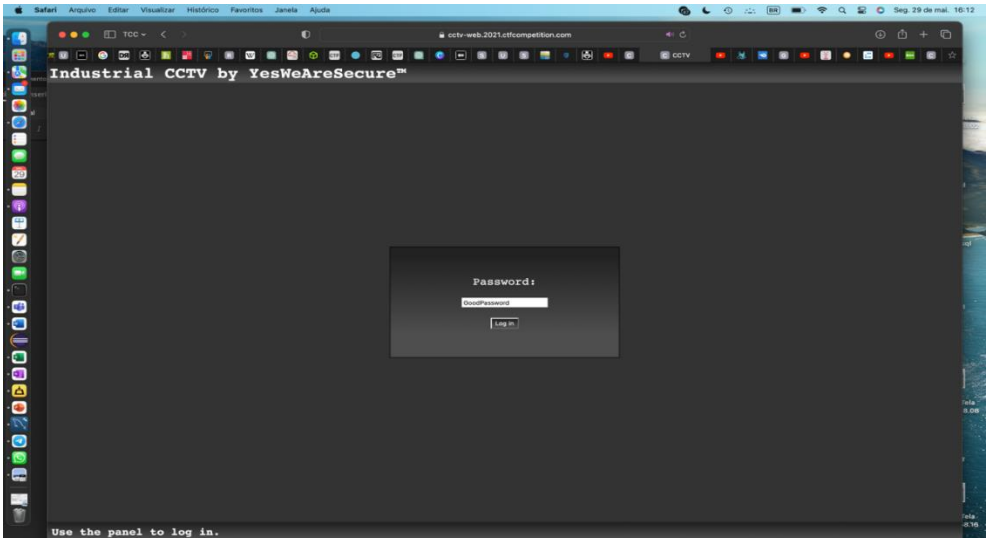
Figura 9- Interface do desafio do GCTF



Fonte: *Screenshot* feita pelo autor

Ao clicar no link ele redireciona para uma nova aba, nesta aba nova sé possível ver que ele está solicitando uma senha para então você poder verificar as câmeras, para descobrir a senha, será necessário inspecionar a página, para verificar o código fonte, e através do código fonte será encontrado uma numeração onde é necessário inserir em um *array* e executar ele em alguma linguagem, então ele dará a senha que se deseja.

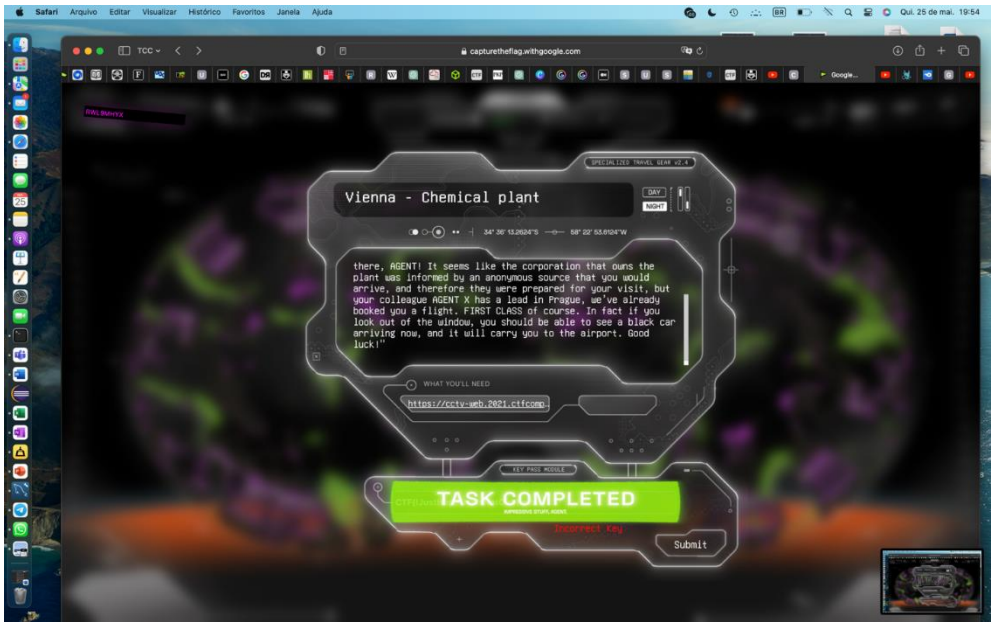
Figura 10- Interface do link disponibilizado no desafio do GCTF



Fonte: *Screenshot* feita pelo autor

Na Figura 12 ele mostra que você conseguiu resolver o exercício dando a mensagem “Task Completed”.

Figuras 12 – interface do desafio do GCTF resolvido



Fonte: *Screenshot* feita pelo autor

Como analisado e demonstrado nas capturas de tela, os exercícios são de criptografia, mas tem também esteganografia no caso da plataforma do google, já na outra plataforma você escolhe qual técnica quer aprender e se desenvolver.

Como demonstrado anteriormente o CTFLEARN e o GTCF são plataformas relacionadas a *Capture the Flag*, onde oferecem recursos e desafios a seus usuários. Por mais que sejam plataformas distintas, elas compartilham o mesmo objetivo final em comum, que é promover a aprendizagem e o desenvolvimento de habilidades em segurança cibernética por meio de desafios e competições.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve como propósito realizar uma descrição pratica das competições de CTF com o intuito de demonstrar sua potencialidade para o desenvolvimento e implementação de plataformas com o uso de C*apture the Flag* dentro de empresas.

Pode-se afirmar que a partir do referencial teórico é percetível a importância e

o valor da ferramenta de *Capture the Flag*, visto que pode auxiliar as indústrias a conquistar mais segurança em seus meios de trabalho.

Considerando que existe algumas razoes bem importantes para as empresas implementarem o *Capture the Flag*, sendo elas, teste de segurança que é onde o ctf permite que as empresas possam avaliar a segurança de seus sistemas, aplicativos e infraestrutura de rede, com os CTF é possível simular os cenários reias de ataques cibernéticos o que irá ajudar as empresas a identificar e corrigir possíveis vulnerabilidades.

Outro ponto muito importante é a que o CTF pode desempenhar u grande papel na conscientização de uma cultura de segurança cibernética, criando uma mentalidade nos profissionais e equipes para que se tornem mais vigilante em relação a possíveis ameaças e melhorem suas boas praticas de segurança.

É importante ressaltar que o CTF deve ser visto como uma parte de uma estratégia abrangente de segurança cibernética nas organizações. Além dos desafios de CTF, é necessário implementar medidas de segurança adequadas, como políticas, treinamentos, testes de penetração e monitoramento contínuo, para garantir uma postura de segurança eficaz.

Por fim, o presente trabalho evidencia que esse tipo de competição pode contribuir para a formação dos acadêmicos, além do aperfeiçoamento das equipes de segurança da informação em organizações, levando em consideração o volume expressivo de ameaças às informações.

REFERÊNCIAS

CHUNG, Kevin; COHEN, Julian. Learning obstacles in the capture the flag model. In: XIV Usemix Summit on Gaming, Games, and Gamification in Security Education, 2014, San Diego, CA. Anais eletrônicos… San Diego, CA: USENIX, 2014. Disponível em: <https://www.usenix.org/conference/3gse14/summit-program/presentation/chung>. Acesso em: 1 maio 2020.

DE OLIVEIRA, Francisco Kelsen et al. ABORDAGENS DE ENSINO PARA SEGURANÇA DA INFORMAÇÃO:: POSSIBILIDADES NOS CURSOS ONLINE ABERTOS E MASSIVOS. Educação Profissional e Tecnológica em Revista, v. 4, n. 1, p. 71-83, 2020.

FAGUNDES, Léa da Cruz et al. Aprendizes do futuro: as inovações começaram. In: FONTES, Edison L. G. (org.). Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GONZALEZ, Hugo; LIAMAS, Rafael; MONTAÑO, Omar. Using CTF tournament for reinforcing learned skills in cybersecurity course. Research in Computing Science, San Luis Potosí, México, 133-141, 2019.

O que é segurança da informação? Disponível em: https://encontreumnerd.com.br/blog/o-que-e-seguranca-da-informacao

Magalhaes, L., Antonio Carlos F. Petri, Gabriel de S. Alves, C. A. C. M., and Matias, P.(2017). Provisionamento automatizado de servidores para competições es de segurança da Informação. XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg 2017

MANSUROV, Alexander. A CTF based approach in information security education: an extracurricular activity in teaching students at Altai State University, Russia. Modern Applied Science, Canadá, v. 10, n. 11, ago. 2016.

MENA, Isabela. Verbete draft: o que é capture the flag (CTF). 7 fev. 2018. Disponível em: <https://www.projetodraft.com/verbete-draft-o-que-e-capture-the-flag-ctf/>. Acessado em: 20 de maio 2023.

PHD DAYS. Phays CTF Over? PHDays CTF Goes On! 20 ago. 2012. Disponível em:<https://www.phdays.com/en/press/news/phdays-ctf-over-phdays-ctf-goes-on/>. Acesso em: 18 mar. 2023.