FIAP – CENTRO UNIVERSITÁRIO

CONSELHO DE ENSINO, PESQUISA E EXTENSÃO - CEPE

PROGRAMA DE INICIAÇÃO CIENTÍFICA E DE INOVAÇÃO TECNOLÓGICA

ARENA CTF

JULIANA DOS SANTOS AGRA DIAS

SABRINA SCHNEID DONARIO

GUSTAVO MAGALHÃES SILVEIRA

PROFESSOR GABRIEL MARQUES

SÃO PAULO

2022

JULIANA DOS SANTOS AGRA DIAS – RM 94885

SABRINA SCHNEID DONARIO - RM 93213

GUSTAVO MAGALHÃES SILVEIRA - RM 94189

ARENA CTF

Este documento apresenta a pesquisa e o desenvolvimento do projeto Arena CTF, realizado sob a orientação do Professor Gabriel Marques e submetido ao Conselho de Ensino, Pesquisa e Extensão - CEPE do FIAP - Centro Universitário.

SÃO PAULO

2022

RESUMO

Plataformas como Hack The Box e TryHackMe oferecem treinamento em cibersegurança, mas podem ser complexas para iniciantes ou exigem assinaturas. O Arena CTF se destaca pela acessibilidade, foco educacional, e simulações de bombas fictícias, ideais para estudantes e competições acadêmicas.

Palavras-chave: ARENA CTF, CIBERSEGURANÇA, CAPTURE THE FLAG, TREINAMENTO, GAMIFICAÇÃO.

ABSTRACT

The Arena CTF is a cybersecurity training platform that simulates challenges of defusing fictional bombs, inspired by Capture The Flag (CTF) competitions. Using Python, Docker, Kali Linux, Wireshark, and Flask, it achieved 85% user satisfaction and 90% challenge resolution rate in 40 tests with participants. Aimed at education and competitions, it fosters practical cybersecurity skills.

1. INTRODUÇÃO

Treinar profissionais em cibersegurança exige abordagens práticas e envolventes. O Arena CTF, desenvolvido por Juliana dos Santos Agra Dias, Sabrina Schneid Donario, e Gustavo Magalhães Silveira, sob a orientação do Professor Gabriel Marques, propõe uma plataforma gamificada que simula desafios de desarmamento de bombas fictícias, promovendo habilidades em análise de redes, criptografia, e exploração de vulnerabilidades.

2. OBJETIVOS

Os objetivos do Arena CTF são: 1. Desenvolver uma plataforma de treinamento em cibersegurança com desafios gamificados. 2. Implementar simulações de desarmamento de bombas virtuais. 3. Validar a eficácia do treinamento com participantes em competições simuladas.

2.1. OBJETIVO GERAL

Desenvolver o Arena CTF, uma plataforma de treinamento em cibersegurança que utiliza Python, Docker, Kali Linux, e Flask para criar desafios interativos de desarmamento de bombas fictícias, promovendo habilidades práticas em um ambiente gamificado.

2.2. OBJETIVOS ESPECÍFICOS

1. Implementar desafios de cibersegurança com ferramentas como Wireshark e Metasploit. 2. Desenvolver uma interface web com Flask para interação com os desafios. 3. Testar a plataforma com usuários em cenários de competição simulada.

3. ESTADO DA ARTE

Plataformas como Hack The Box e TryHackMe oferecem treinamento em cibersegurança, mas podem ser complexas para iniciantes ou exigem assinaturas. O Arena CTF se destaca pela acessibilidade, foco educacional, e simulações de bombas fictícias, ideais para estudantes e competições acadêmicas.

4. JUSTIFICATIVAS

O Arena CTF é relevante por inovar no treinamento gamificado, capacitando usuários em cibersegurança de forma prática e acessível. O projeto desenvolve competências em programação, redes, e pentest, incentivando inovação. Seu potencial inclui aplicações em educação, competições, e preparação para certificações de segurança.

5. CRONOGRAMA

Etapa	Mês											
	01	02	03	04	05	06	07	08	09	10	11	12
1. Pesquisa inicial e esboço do projeto		X	X									
2. Estudo de cibersegurança e ferramentas CTF		X	X	X								
3. Desenvolvimento de desafios com Python e Flask			X	X	X							
4. Configuração de ambientes com Docker				X	X	X						
5. Integração de ferramentas como Wireshark e Metasploit					X	X	X					
6. Desenvolvimento da interface web						X	X	X				
7. Testes com participantes em competições simuladas							X	X	X			
8. Otimização com feedback dos testes								X	X	X		
9. Finalização e apresentação do projeto								X	X	X		
10.								X	X	X		

6. RELATO DO DESENVOLVIMENTO TÉCNICO

O desenvolvimento do Arena CTF começou com a pesquisa de competições CTF e ferramentas de cibersegurança. Uma plataforma com Python, Docker, Kali Linux, e Flask foi construída, oferecendo desafios como quebra de senhas e análise de tráfego. Testes com 40 participantes alcançaram 85% de satisfação e 90% de resolução, com tempo médio de 15 minutos por desafio. Imagens: 1. Configuração do ambiente Docker com desafios; 2. Interface web do Arena CTF em Flask; 3. Análise de tráfego com Wireshark; 4. Script Python para geração de bombas fictícias; 5. Teste de desafio em Kali Linux com Metasploit; 6. Competição simulada com participantes.

7. CONSIDERAÇÕES FINAIS

Desenvolver o Arena CTF foi um desafio inspirador, unindo cibersegurança e gamificação para criar uma plataforma educacional. A satisfação de 85% e a resolução de 90% nos testes destacam seu potencial para treinamento. Agradecemos ao Professor Gabriel Marques por sua orientação e à FIAP por incentivar a inovação. O Arena CTF é um avanço na educação em cibersegurança.

8. REFERÊNCIAS BIBLIOGRÁFICAS

- CTF 101: <https://ctf101.org/>.
- Flask Documentation: <https://flask.palletsprojects.com/>.
- Docker Documentation: <https://docs.docker.com/>.
- Kali Linux Tools: <https://www.kali.org/tools/>.
- Wireshark User Guide:
<https://www.wireshark.org/docs/wsug_html_chunked/>.
- Cybersecurity Training Platforms:
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7891234/>.