Gamificação como uma abordagem ao ensino de redes de telecomunicações e segurança cibernética: Telecom Challenge

Luiz F. F. Irineu, Vitória M. Dutra, Francisco A. S. do Carmo, Marcelo O. Marques, Evandro C. Vilas Boas
Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações - Inatel
luizirineu@get.inatel.br, vitoria.dutra@gea.inatel.br, francisco.assis@inatel.br, marcelo@inatel.br, evandro.cesar@inatel.br

***Abstract*—This article presents the Telecom Challenge project on gamification to teach fundamental telecommunications networks and cybersecurity principles. This innovative methodology engages students, developing skills and competencies in the related area. The Telecom Challenge project is based on a Capture the Flag (CTF) style competition, where students must solve challenges presented through an online platform assertively in the shortest possible time. The projects second edition brought together around 250 students from Minas Gerais, São Paulo, and Rio de Janeiro secondary and technical schools.**

***Index Terms*—Teaching, cyber security, gamification, innovation, Telecommunication.**

***Resumo*—Esse artigo apresenta o projeto Telecom Challenge - Desafio Hacker desenvolvido com base em gamificação como uma abordagem ao ensino de redes de telecomunicações e cyber segurança. Emprega-se a gamificação aplicada ao ensino tradicional como forma de desenvolvimento de metodologias inovadoras, buscando estimular a participação de alunos em diversas atividades para desenvolver habilidades e competências na área correlata. O projeto Telecom Challenge baseia-se em uma competição estilo *Capture the Flag* (CTF) em que alunos devem solucionar desafios por meio de uma plataforma online de forma assertiva e no menor tempo possível. Em sua segunda edição, o projeto reuniu cerca de 250 alunos de escolas de ensino médio e/ou técnico dos estados de Minas Gerais, São Paulo e Rio de Janeiro.**

***Palavras chave*—Ensino, cyber segurança, gamificação, inovação, Telecomunicações.**

I. Introdução

A gamificação ou *gamification* é uma prática que utiliza elementos de jogos como ferramentas de engajamento para atingir determinado objetivo em diversas áreas como, por exemplo, a educação ou negócios [1]. No ensino, essa prática tornou-se útil para o engajamento e aprendizado de jovens e adolescentes devido ao seu alto potencial em despertar interesse, estimular o trabalho em equipe, desenvolver criatividade e autonomia, promover diálogo e um *feedback* instantâneo do aprendizado [1, 2]. Aplicam-se jogos como metodologias para o aprendizado, tornando a assimilação de conteúdo prazerosa e intuitiva. Essa prática encontra-se em evidência e desenvolvimento, dado o contexto atual, em que o acesso à dispositivos eletrônicos têm-se popularizado. Dessa forma, a realização de competições tecnológicas, relacionadas as mais diversas áreas, visa motivar o aluno, tornando-se um meio para o aprendizado e popularização do conhecimento correlato. Esses eventos também permitem a inclusão social de jovens e adolescentes à um mundo cada vez mais digitalizado.

Portanto, o Instituto Nacional de Telecomunicações (Inatel), por meio da Coordenação de Engenharia de Telecomunicações e Núcleo de Relacionamento de Colégios, desenvolveu o projeto Telecom Challenge – Desafio Hacker. Esse projeto tem como objetivo disseminar o conhecimento na área de redes de telecomunicações e cyber segurança por meio de uma competição para alunos de ensino médio e/ou técnico de escolas públicas e particulares. Estrutura-se o evento em fase preparatória, onde os alunos recebem materiais didáticos, conteúdo audiovisual e tutoria no aprendizado de aspectos relacionados a redes de telecomunicações e cyber segurança. Em uma segunda etapa, tem-se o desenvolvimento de uma competição que visa reforçar o aprendizado por meio de jogos em grupos e individuais em uma plataforma on-line. Além disso, o projeto também contribui para a instrução desse público sobre boas práticas em segurança cibernética, refletindo em seu desenvolvimento pessoal e profissional.

Esse trabalho apresenta um panorama geral do projeto Telecom Challenge - Desafio Hacker e encontra-se estruturado em quatro seções. Na Seção II, apresentam-se os conceitos básicos em telecomunicações e segurança cibernética, que são abordados na competição. Discutem-se a estrutura e etapas do projeto Telecom Challenge na Seção III. Assim como, apresenta-se a plataforma de competição online. Conclusões e comentários finais encontram-se na Seção IV.

II. Fundamentos em Telecomunicações e Cyber Segurança

No projeto, abordam-se como conteúdos quatro temas macro: introdução às telecomunicações, introdução as redes de computadores, conceitos básicos de protocolos de rede, redes Ethernet e WiFi e fundamentos de segurança cibernética. Em introdução às telecomunicações, discutem-se os princípios e elementos básicos de uma telecomunicação, tipos de telecomunicação e meios físicos. Esse conhecimento é base para a compreensão dos módulos posteriores.

Em introdução as redes de computadores e Internet, apresentam-se os conceitos e elementos básicos, tipos de redes de computadores e classificações, topologias físicas de redes, arquiteturas de redes em camadas (ex.: Modelo OSI - *Open System Interconnection*) e tráfego de informações pela rede [3]. Demonstram-se os conceitos básicos em protocolos de rede e discutem-se protocolos como DHCP (*Dynamic Host Configuration Protocol*), ARP (*Address Resolution Protocol*) e DNS (*Domain Name System*).

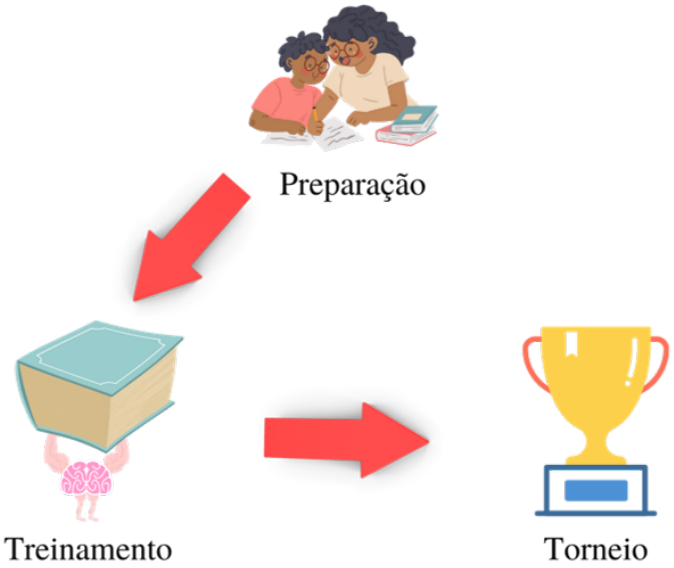

Fig. 1. Estrutura do projeto Telecom Challenge.

Estudam-se as principais características das redes Ethernet e WiFi como forma de demostrar aos participantes como as redes de telecomunicações estão presentes no dia-a-dia das pessoas garantindo a conectividade à Internet. Por fim, introduzem-se os fundamentos de cyber segurança como seus pilares, os tipos de ataques em que uma pessoa ou empresa esta venerável, a definição de *Pentester* e *Ethical Hacker*, finalizando assim o conteúdo programático para que os participantes possam participar da competição [4, 5].

III. Projeto Telecom Challenge

Nessa seção descreve-se a estrutura do projeto Telecom Challenge. Assim como, apresenta-se a plataforma de competições online CTFd.io [6]. O projeto Telecom Challenge compreende duas categorias: individual e em grupo.

A. Estruturação

Estrutura-se o projeto em etapas que compreendem a preparação, treinamento e torneio, conforme ilustrado na Fig. 1. A preparação tem como objetivo introduzir os conceitos discutidos na Seção II. Dessa forma, os alunos recebem material didático em formato de apostilas que contemplam quatro capítulos: Introdução às Telecomunicações, introdução as redes de computadores, conceitos básicos em protocolos, redes Ethernet e WiFi e fundamentos de cyber segurança. Além do material didático, ofertam-se cursos em formato online para apresentação e discussão desses assuntos de forma a prover melhor compreensão. Meios audiovisuais como vídeos de curta duração são disponibilizados na plataforma You Tube para que os participantes possam acessá-los e revisar o conteúdo. Ao fim da etapa de preparação, apresentam-se algumas ferramentas de criptografia básica como, por exemplo, cifras de César e texto cifrado. Empregam-se essas ferramentas para a elaboração dos desafios das fases seguintes.

Na etapa de treinamento, oferecem-se competições, em grupos e individual, que tem como objetivo fixar o aprendizado por meio de jogos em uma plataforma on-line que permite a interação entre os alunos. Durante o treinamento, os alunos tem a oportunidade de conhecer a plataforma e suas diversas funcionalidades, treinar os conhecimentos adquiridos durante a preparação, assim como compreender a dinâmica do torneio. Por fim, estrutura-se um torneio para as categorias individual e em grupo, sendo composto por fases eliminatórias e final. Nas fases eliminatórias, os participantes jogam com o objetivo de acumular pontos para se classificar para a final. Nessa fase, definem-se os ganhadores de cada categoria em uma única competição, respectivamente.

B. Plataforma de competição CTFd.io

Para gamificar o aprendizado dos participantes e estimulá-los a participar das atividades de ensino, utilizou-se a plataforma on-line CTFd.io [6], cuja interface inicial é vista na Fig. 2. Essa plataforma permite a competição em caráter on-line tanto nas categoria individual quanto em grupo, viabilizando a exequibilidade e abrangência geográfica do projeto.

A plataforma baseia-se em competições no estilo *Capture the Flag* (CTF), apresentando ao participante desafios dentro de uma temática, no caso, telecomunicações e segurança cibernética. Para obter a pontuação e o melhor posicionamento no *rank*, deve-se fornecer a resposta de forma correta no menor tempo possível em relação ao início da competição.

Para o projeto, as resposta assumem formatos diversos para trabalhar de forma alusiva aspectos de cyber segurança. Dessa forma, exploram-se as funcionalidades *case sensitive* e *case insensitive*. A primeira permite restringir o formato da resposta pela diferenciação de maiúsculas e minúsculas. Já o segundo tipo não faz nenhuma distinção. No contexto do projeto, manipulam-se as respostas por meio de ferramentas básicas de criptografia disponíveis online. A plataforma também permite ofertar dicas para a solução dos desafios ao custo de uma parcela da pontuação acumulada. Logo, estimula-se, além de conhecimentos técnicos, outras competências como a administração de recursos e riscos, inerentes aos projetos de engenharia.

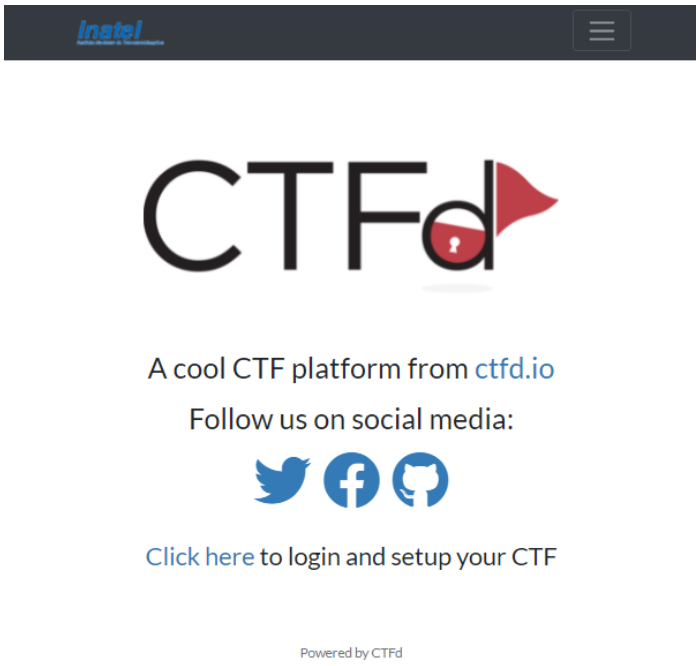

Fig. 2. Paltaforma CTFd.io utilizada no projeto Telecom Challenge.

C. Público-alvo e edições do Telecom Challenge

O projeto Telecom Challenge tem como foco alunos de ensino médio e técnico de escolas públicas e particulares do Brasil e encontra-se em sua segunda edição. Na primeira edição, o projeto reuniu cerca de 130 alunos nas categorias individual (92 participantes) e em grupo (60 participantes). Na segunda edição, 250 alunos se inscreveram, sendo 118 participantes na categoria individual e 173 na categoria em grupo. Observa-se aumento na capitação de participantes, oriundo da disseminação da competição por membros que participaram da primeira edição e maior engajamento das escolas em agregar o projeto ao calendário letivo.

IV. Conclusão

Esse trabalho apresentou o projeto Telecom Challenge, como um exemplo de gamificação dos estudos relacionados às telecomunicações e segurança cibernética. Demonstrou-se a estrutura desenvolvida com base em três etapas: capacitação, treinamento e competição. Verificou-se que a gamificação desempenhou importante papel no engajamento dos participantes, comprovando-se um método eficaz para disseminação de conhecimentos em Telecomunicações e Engenharia à alunos de escolas públicas e particulares da região sudeste do Brasil. Como trabalhos futuros, visa-se estruturar as competições em torno de uma temática, permitindo desenvolver uma narrativa (*storytelling*) como forma de aumentar o engajamento dos alunos e atrair maior público.

Agradecimentos

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio na execução das atividades propostas, ao Instituto Nacional de Telecomunicações (Inatel) e ao Laboratório de Segurança Cibernética e Internet das Coisas (CS&I Lab.) por todo o suporte técnico oferecido.

Referências

[1] B. V. Tomolei. "A Gamificação como Estratégia de Engajamento e Motivação na Educação". Em: *Revista Cientìfica do Ensino à Distância (EaD em Foco)* 2.7 (2017), pp. 145–156. DOI: 10.18264/eadf.v7i2.440.

[2] J. de A. Santos e A. L. C. Freitas. "Gamificação Aplicada a Educação: Um Mapeamento Sistemático da Literatura". Em: *RENOTE – Revista Novas Tecnologias na Educação* 1.15 (2017), pp. 1–10. DOI: 10.22456/1679-1916.75127.

[3] J. Kurose e K. Ross. *Redes de computadores e a Internet: Uma abordagem top-down*. São Paulo: Person Education do Brasil, 2013.

[4] W. Stallings. *Criptografia e Segurança de Redes*. São Paulo: Person Education do Brasil, 2008.

[5] S. McClure, J. Scambray e G. Kurtz. *Hackers expostos: segredos e soluções para a segurança de redes*. Porto Alegre: Bookman, 2014.

[6] CTFd. *CTFd: The Easiest Capture the Flag Plataform*. . [Online]. Disponível em: https://ctfd.io/features/. Acesso: 17.08.2021.