UNIVERSIDADE FEEVALE

LUCAS HENRIQUE DE MORAES

CTF: Um Estudo teórico e prático para construção de conhecimento na área de segurança da informação

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo
2020

LUCAS HENRIQUE DE MORAES

CTF: Um Estudo teórico e prático para construção de conhecimento na área de segurança da informação

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale

Orientador: Dr. Daniel Dalalana Bertoglio.

Novo Hamburgo
2020

RESUMO

O tema de segurança da informação tem se tornado comum no dia a dia das pessoas, pois tanto em seus locais de trabalho onde grande parte das informações da organização estão armazenadas em um ambiente computacional quando em seus computadores e celulares onde utilizam diversos aplicativos para movimentações bancárias e trocar de mensagens. Nas organizações esse tema tem ganhada cada notoriedade, devido as informações serem consideradas como ativos de valor, que contribuem para alcançar seus objetivos e missões. Dentro desse ambiente surge a necessidade de profissionais na área de sprepara egurança de informação cada vez mais capacitados para lidar com os desafios que devem enfrentar diariamente, onde não basta somente o conhecimento teórico das técnicas de segurança da informação, sendo necessários treinamentos práticos. Dentro desse cenário é apresentado o CTF como ferramenta para contribuir na construção de conhecimento e habilidades, tendo em vista que as competições nesse âmbito instigam os participantes a buscar novas técnicas, contribuindo com o crescimento da área. Baseado nisso o presente trabalho visa estudar as principais técnicas utilizadas em CTF com o intuito de desenvolver habilidades relacionados ao conteúdo de segurança da informação. Dessa forma esse estudo é norteado pela seguinte questão de pesquisa: “Como auxiliar os profissionais no desenvolvimento de conhecimentos na área da segurança da informação através de práticas de CTF e técnicas relacionadas nesse contexto!”.

Palavras-chave: CTF. Cibersegurança. Habilidades. Desenvolvimento. Competição.

SUMÁRIO

MOTIVAÇÃO

O tema de segurança da informação tem se tornado comum no dia-a-dia das pessoas, pois tanto em seus locais de trabalho onde grande parte das informações da organização estão armazenadas em um ambiente computacional quando em seus computadores e celulares onde utilizam diversos aplicativos para movimentações bancárias e trocar de mensagens. (FONTES, 2006).

As organizações têm procurado um diferencial em suas organizações frente aos concorrentes, e tem encontrado soluções em na área de TI, que tem oferecido ferramentas facilitam a tomada de decisão baseada em informações úteis e atuais, e também transformando tais informações em conhecimento, sendo o conhecimento uma grande vantagem competitiva dentro das organizações (NONAKA; TAKEUCHI, 2009).

Sendo a informação um dos principais ativos, as organizações têm sido expostas à ameaças, gerando a necessidade de garantir a segurança da informação, através de softwares de seguranças (antivírus, softwares de detecção de intrusão), Ferreira (1994) observa que "a capacidade competitiva de uma empresa está intimamente relacionada à conjugação de gestão e informação tecnológica, devido às crescentes exigências do mercado com relação a novos produtos e serviços de alto conteúdo tecnológico".

Fontes (2006) complementa o pensamento falando que informação devem ser cuidadas da mesma maneira que as organizações tem com os recursos financeiros, pois a mesma é um ativo de valor, pois a mesma auxilia na execução das missões e objetivos da empresa, analisando que o bem de maior valor da organização está disponível em grandes bancos de dados ou arquivos, surge a necessidade de protegê-las com os demais ativos. Conforme reportagem da Computer World (2019), todos os dias organizações sofrem ataques de hackers maliciosos, dessa forma, gerando prejuízos financeiros, interrupção de serviços e até mesmo impacto na imagem frente ao mercado.

Dentro desse ambiente surge a necessidade de profissionais na área de segurança de informação. Trickel et al. (2017) descreve uma possível crise, pois a necessidade de profissionais qualificados é insuficiente para atender a demanda do mercado. Desse modo, entende-se que o estudo teórico não seja o suficiente para preparar os profissionais para enfrentar o atual cenário, e considera a prática como aspecto crucial para entender a complexidade da segurança cibernética. Nakaya et al. (2016) contribui com a ideia no sentido que mesmo com seminários e cursos os profissionais tendem a perder o interesse e a

motivação pelo estudo das práticas de segurança devindo, principalmente, aos altos custos para elaboração de práticas em ambiente real.

Boopathi et al. (2015) fez uma relação entre dados de uma pesquisa do órgão CERT (Computer Emergency Report Team) sobre o grande número de domínios comprometidos devido ações de hackers maliciosos e a capacidade dos desenvolvedores e profissionais na atualidade referente as práticas de segurança da informação. Neste estudo, corroborando com os autores previamente citados, Boopathi constatou uma possível lacuna nas questões práticas ao revisar o currículo das graduações e de pós-graduações do local da pesquisa. Com base nisso, o autor propõe uma solução de treinamento utilizando a "capture a bandeira" ou CTF, do inglês, Capture The Flag.

Capture The Flag é uma modalidade de competição de cibersegurança, onde os competidores devem dispor de um conhecimento amplo de técnicas da área de segurança, como criptografia, redes, programação, *cloud computing*, *pentest*, engenharia reversa, exploração de binários, análise forense, estenografia com o objetivo de capturar a bandeira, que pode ser um trecho de código ou até mesmo uma mensagem. (GONZALEZ et al., 2019)

As competições podem correr em três (3) modalidades, sendo que cada uma das modalidades pode ser realizada individualmente ou em equipe. Segundo Seltzer (2019), os estilos estão propostos da seguinte maneira:

Ataque e Defesa - Consiste em duas equipes, cada uma com um ambiente computacional preparado, e pode ocorrer de forma online e/ou local. Nessa modalidade, cada equipe tenta realizar ataques ao sistema do outra e defender o seu. Nessa modalidade de competição as equipes de defesa podem preparar seus sistemas como desejar, corrigindo todas as vulnerabilidades deixando somente os serviços necessários abertos no firewall. Em contrapartida, os atacantes utilizam técnicas de intrusão para obter privilégios e informações.

Jeopardy - Essa modalidade é baseada em quizzes (questionários) que são divididos em níveis de dificuldades, e cada desafio tem valores diferentes de pontuação. Assim, cada acerto leva uma determinada pontuação e ao próximo nível. Ao final de um tempo determinado, a equipe que tiver a maior pontuação vence.

King of the hill (Rei da Montanha) – Nessa modalidade é apresentado para as equipes um determinado servidor onde devem assumir o controle. Após o final do período, estipulado a equipe que teve o maior controle do serviço por mais tempo vence.

Segundo Eagle e Clark (2004) e Mansurov (2016) o CTF contribui com a aquisição de novas habilidades para profissionais de cibersegurança, habilidades cujo os currículos

padrões não têm oferecido, tendo em vista que as competições nesse âmbito instigam os participantes a buscar novas técnicas de conhecimento na área, contribuindo para sanar a demanda do mercado.

Para Eagle e Clark (2004) o CTF no estilo de ataque e defesa pode contribuir na aquisição de novas habilidades para profissionais da área, habilidades cujo nenhum currículo padrão educacional tem para oferecer, uma vez que esse esporte oferece uma liberdade que inspira os participantes a aprimorar suas técnicas.

Compreende-se então que essas competições podem auxiliar o desenvolvimento de habilidades e conhecimentos dos participantes, e assim contribuir com a área de segurança da informação (MANSUROV, 2016).

Baseado nisso o presente trabalho visa estudar as principais técnicas utilizadas em CTF com o intuito de desenvolver habilidades relacionados ao conteúdo de segurança da informação. Dessa forma esse estudo é norteado pela seguinte questão de pesquisa: “Como auxiliar os profissionais no desenvolvimento de conhecimentos na área da segurança da informação através de práticas de CTF e técnicas relacionadas nesse contexto!”.

OBJETIVOS

Objetivo geral

Desenvolver um estudo teórico e prático sobre técnicas utilizadas em CTF para construção de conhecimento e habilidades relacionadas a Segurança da Informação por parte de alunos.

Objetivos específicos

- Identificar e analisar a contribuição de CTF na evolução de alunos/profissionais de cibersegurança;
- Estudar e compreender as competições de CTF;
- Realizar um levantamento das principais técnicas utilizadas em CTF;
- Demonstrar a necessidade de capacitação dos profissionais;
- Desenvolver uma competição de CTF com alunos;
- Analisar os resultados de cada etapa da competição.

METODOLOGIA

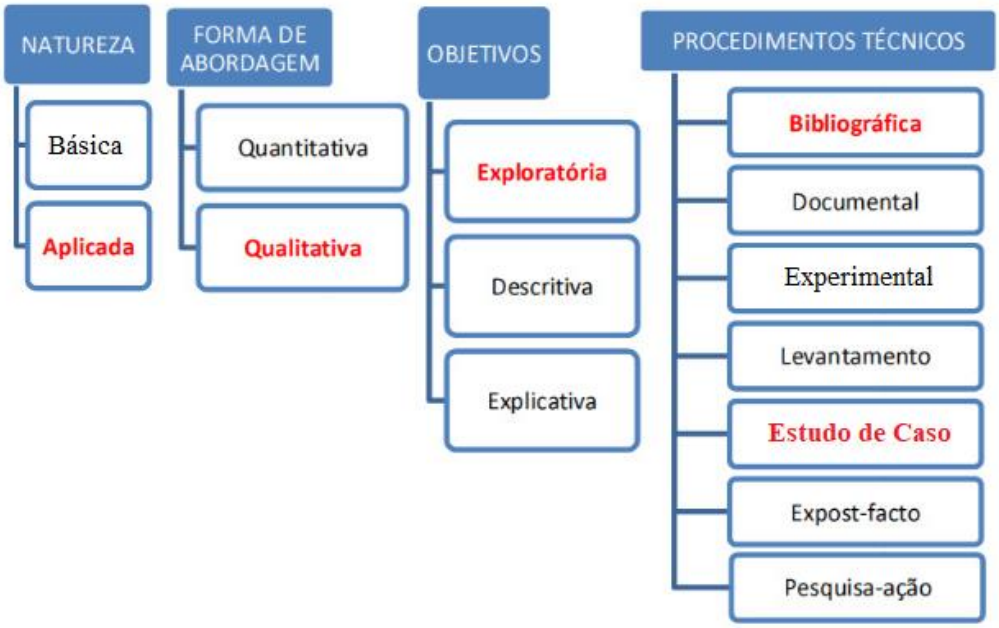

Figura 1 - Classificação da pesquisa (adaptado de BEZ, 2011)

O presente trabalho caracterizasse como uma pesquisa aplica, pois tem o objetivo de gerar conhecimento, elaborando um estudo referente à CTF para contribuir para geração de conhecimento e habilidades para alunos e profissionais da área de segurança da informação.

A forma de abordagem será qualitativa, pois através da análise de especialistas buscar-se-á uma ampla compreensão de como o CTF pode contribuir na construção de conhecimento e habilidades que podem ser utilizadas diariamente nas organizações.

Os objetivos deste trabalho podem caracteriza-lo como uma pesquisa do tipo exploratória, pois foca no estudo de determinada área de ação, suas premissas e necessidades para que, a partir disso, possa ser desenvolvido um treinamento do conhecimento adquirido para auxiliar na construção de novos conhecimentos e habilidades.

Quanto aos procedimentos técnicos, considera-se o trabalho como bibliográfico e estudo de caso. O procedimento bibliográfico será realizado através de pesquisas em trabalhos acadêmicos, artigos, publicações e manuais referente CTF. O levantamento bibliográfico servirá como base para a definição da proposta de treinamento que possa auxiliar no processo de obtenção de conhecimento e técnicas para alunos e profissionais.

O estudo de caso se dará na aplicação do conhecimento adquirido com o levantamento bibliográfico dentro de uma realidade circunstancial, onde será aplicado sobre um grupo ou comunidade de alunos e profissionais da área de segurança de informação, procurando elucidar a motivação dessa pesquisa, que consiste em analisar a contribuição do CTF no desenvolvimento de conhecimento e habilidades na área de cibersegurança.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	Mar	Abr	Mai	Jun
Estudo sobre CTF e cibersegurança				
Desenvolver e entregar o Anteprojeto				
Aprofundar o estudo de CTF				
Desenvolver e entregar o Trabalho de Conclusão I				

Trabalho de Conclusão II

Etapa	Meses			
	Ago	Set	Out	Nov
Elaborar e aplicar competição de CTF				
Analisar o resultado da primeira etapa				
Aplicar a segunda competição de CTF				
Desenvolver o Trabalho de Conclusão II				

BIBLIOGRAFIA

BOOPATHI, K.; BITHIN, S. S. A. A. **Learning Cyber Security Through Gamification**, Amritapuri, Índia, v. 8, p. 642-649, 2015.

EAGLE, Chris; Clark, John L**. Capture-the-flag**: LEARNING COMPUTER SECURITYUNDER FIRE, Monterey, Califórnia, 2004. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a435319.pdf>. Acesso em: 10 de março de 2020.

FERREIRA, J.R. - **Informação é instrumento essencial para a competitividade na indústria**, TECBAHIA, Camaçari, v.9, n.3, p.5-6, 1994.

FONTES, Edison**. 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**, San Luis Potosí, SLP, México, 2019.

MANSUROV, Alexander. **A CTF based approach in information security education**: An extracurricular activity in teaching students at altai state university, Russia, Barnaul, 2016. Disponível em: <https://pdfs.semanticscholar.org/8a56/cad25bbc560f31e595d2504c399363e18e7b.pdf>. Acesso em: 10 de março de 2020.

NAKAYA, Makoto; ABE, Takayuki; TOMINAGA, Hiroyuk**. Implementation and trial practices for hacking competition CTF as introductory educational experience for information literacy and security learning**. Kagawa, Japão, 2015.

NONAKA, I.; TAKEUCHI, H. **Gestão do conhecimento**. Porto Alegre: Bookman, 2009.

SELTZER, Larry. **Top tools and resources for running a capture the flag competition** , 2019 , Disponível em: <http://www.biblioteca.fsp.usp.br/~biblioteca/guia/a_cap_03.htm> .Acesso em 7 de março.

TRICKEL, E. et al. **Shell We Play A Game?:** CTF as a service for security education , Arizona ,2017. Disponível em: <https://www.usenix.org/system/files/conference/ase17/ase17_paper_trickel.pdf>. Acesso em: 10 de março de 2020.