Uma abordagem para gestão de cenários no ensino de Segurança de Sistemas de Informação

Rafael Vinícius Barros Ferreira, Bruno P. T. Freitas, Nilson M. Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

rafael.ferreira@aluno.cefet-rj.br, {bruno.freitas,nlazarin}@cefet-rj.br

Abstract. *Training qualified professionals to work in Information Systems Security (ISS) is essential to meet the needs of organizations that need data and systems protection. The emphasis solely on the theoretical content of SSI (Information Systems Security) courses and the lack of proper preparation to deal with security are some of the reasons pointed out by graduates of higher education courses. These factors impact the non-implementation of cyberattack prevention techniques in their applications. This work proposes an approach for managing attack scenarios and cybernetic defense to be used in practical ISS classes by defining network environments containing assets of layers 2, 3, and 7 of the ISO/OSI model.*

Resumo. *A formação de profissionais capacitados para atuarem na área de Segurança de Sistemas de Informação (SSI) é de suma importância para atender a necessidade das organizações que necessitam de proteção de dados e sistemas. A ênfase somente no conteúdo teórico das disciplinas de SSI e a falta de uma preparação adequada para lidar com segurança, são alguns dos motivos apontados por egressos de cursos superiores, que impactam na não implementação de técnicas de prevenção de ataques cibernéticos em suas aplicações. Este trabalho propõe uma abordagem para gestão de cenários de ataque e defesa cibernética para serem utilizados em aulas práticas de SSI, através da definição de ambientes de rede contendo ativos das camadas 2, 3 e 7 do modelo ISO/OSI.*

1. Introdução

Segurança de Sistemas da informação (SSI) é um tema cada vez mais relevante em uma cibersociedade. A formação de profissionais capacitados para atuarem nesta área é imprescindível, dada a crescente demanda por proteção de dados. Todavia, muitos egressos de cursos superiores relatam uma lacuna na preparação adequada para lidar com questões de SSI [Cristani et al. 2020]. A falta de preparo afeta diretamente na implementação de técnicas de prevenção de ataques cibernéticos em seus projetos [Costa et al. 2018]. Em meio ao aumento de ciber risco, é necessário que os profissionais da área de SSI sejam capacitados a enfrentar os desafios e proteger os ativos das organizações [Dantas 2022].

A motivação surge da identificação de um problema no processo de aprendizado em SSI. Alunos enfrentam dificuldades em acessar ambientes práticos e interativos que auxiliem no aprimoramento de habilidades. A escassez de recursos e ambientes controlados restringe a aplicação dos conceitos teóricos. Além disso, restrições de tempo dificultam a realização de atividades práticas, pois a preparação do cenário é uma tarefa longa e

suscetível ao erro, podendo se estender ainda mais dependendo da quantidade de alunos na matriculados na disciplina. Essas limitações afetam negativamente a experiência de aprendizado.

Nesse cenário, esse trabalho propõe uma abordagem para orquestração de cenários de ataque e defesa cibernética para o ensino de SSI, criando assim um ambiente de *Cyber Range* baseado em um cluster de alta disponibilidade utilizando o Proxmox. Esses ambientes virtualizados incorporam, sistemas operacionais, redes e ativos de diferentes camadas do modelo ISO/OSI, oferecendo aos estudantes um ambiente de treinamento realista e prático. Dessa Maneira, os alunos são capacitados e desenvolvem habilidades substanciais para atuarem na área de SSI.

Cyber Range é um ambiente simulado com o propósito de treinar e testar habilidades em segurança cibernética, permitindo a criação de cenários de treinamentos virtualizados e controlados para a simulação de exercícios práticos de ataque e defesa [Dantas 2022]. Estratégias de virtualização e acesso remoto tem sido adotadas para viabilizar o ensino prático de disciplinas da área de redes [Bressan et al. 2022] e abordagens baseadas em casos tem contribuído para o processo de ensino/aprendizagem em segurança cibernética [da Silva Melo and Oliveira 2020].

O Proxmox é um ambiente de virtualização de código aberto com interface web intuitiva e arquitetura flexível. Ele otimiza suporte para hypervisors KVM e Linux Containers (LXC), permitindo administração prática via web ou CLI. Gerencia clusters de alta disponibilidade, facilita migrações online, oferece serviços integrados como firewall, backup, restauração e replicação de armazenamento. Sua licença de código aberto proporciona liberdade e flexibilidade, com opção de suporte especializado para necessidades empresariais [Proxmox GmbH 2023].

A relevância deste trabalho é contribuir com o ensino, a pesquisa e a extensão universitária em SSI. através da criação de tecnologia que facilite a orquestração de ambientes seguros para o exercício de ataque e defesa cibernética que permitam o teste de hipóteses e de melhorias para a área de SSI. Atavés do uso do cluster de alta disponibilidade. Esse ambiente poderá ser executado em um ambiente on-premise(localmente em servidores da organização) ou uma private cloud, permitindo assim que as instituições de ensino possam utilizar a solução da forma que melhor se adequá aos seus cenários e recursos minimizando os seus custos. Assim, os alunos praticarão situações reais em ambiente seguro.

Este trabalho está organizado da seguinte forma: na Seção 2 são apresentados alguns trabalhos relacionados; na Seção 3 é apresentada a proposta deste trabalho; na Seção 4 uma discussão é apresentada.

2. Trabalhos relacionados

Realizou-se uma pesquisa bibliográfica com o objetivo de obter embasamento técnico e teórico sobre cibersegurança, virtualização, hypervisor e o ensino por meio de simuladores. Essa etapa foi essencial para compreender o estado atual do conhecimento e identificar lacunas ou oportunidades de pesquisa. Para tal foi definida uma string[1] de busca que

[1](“segurança de sistemas” OR “cibersegurança”) AND (“virtualização” OR “simulação”) AND “ensino” AND (“ferramenta” OR “plataforma”)

foi utilizada no Google Schoolar, que retornou 758 resultados. Após, foi realizada uma análise seguindo os seguintes critérios de aceitação:

- Artigos ou trabalhos publicados de 2016 em diante.
- Artigos ou trabalhos que o título tenha relação com segurança de SSI.
- Artigos ou trabalhos que o resumo tenha relação com o tema escolhido.
- Artigos ou trabalhos que a proposta e o objetivo tivesse relação com o tema escolhido

Em *CyRIS: A Cyber Range Instantiation System for Facilitating Security Training* [Pham et al. 2016], é apresentada uma solução para o desafio de criar ambientes virtuais controlados e bem definidos para o treinamento em segurança cibernética. O CyRIS é um sistema que possibilita a preparação e o gerenciamento automatizado de cyber ranges, com base em especificações fornecidas pelos instrutores. O trabalho aborda o design, a implementação e a utilização da solução, além de discutir os resultados de desempenho obtidos em diferentes cenários representativos.

Em *CyRM: cyber range para auxiliar o ensino de defesa para alunos da disciplina de segurança da informação* [Dantas 2022], é apresentada uma ferramenta para treinamento e capacitação em segurança cibernética, utilizando Containernet[2], um software capaz de emular a topologia da rede. Além disso, são empregados containers Docker para fornecer serviços e ataques previamente definidos.

Em *Firewall GNU/linux e IP tables: um estudo de implementação de ensino no plano de disciplina da formação do oficial de carreira de comunicações* [Pereira 2019], é apresentada uma avaliação da necessidade e viabilidade do ensino prático de firewall. A pesquisa revelou que muitos alunos têm conhecimento insuficiente sobre firewalls e não se sentem preparados para configurá-los. Foi constatada a necessidade de modificações no plano de disciplina para abordar o assunto de forma mais específica e progressiva.

Este trabalho, diferente de Pham et al. (2016), apresenta uma abordagem que busca construir cenários em clusters de alta disponibilidade, possibilitando cenários de rede mais complexos e distribuídos. Diferente de Dantas (2022), os cenários propostos neste trabalho, não são baseados em dockers e sim em virtualização completa de SO, permitindo simulações mais realistas e o uso de distribuições especializadas para o ensino de segurança, tal como o Metasploitable[3] e o Kali Linux[4]. Por fim, será realizada uma análise de aceitação de tecnologia, focado nos docentes responsáveis por disciplinas de SSI, buscando avaliar a possibilidade de inclusão da metodologia em atividades práticas de disciplinas de SSI, diferentemente do realizado por Pereira (2016).

3. Proposta

Esse trabalho propõe criar um CyberRange, construindo um *interpretador de cenários*, nesse contexto assumindo a forma de *API (Application Programming Interface)*, destinada a receber mapeamento de cenários elaborados pelos usuários e enviados para API em formato JSON(JavaScript Object Notation). Ele desempenhará a função de interpretador de cenários, encarregando-se de gerar todo o manifesto necessário para a criação

[2]`https://containernet.github.io/`
[3]`http://metasploitable.sf.net`
[4]`https://www.kali.org/`

e configuração das máquinas virtuais. Adicionalmente, terá a capacidade de se comunicar com a API do Proxmox para o gerenciamento completo do ambiente por CLI, configurações de rede, criação, destruição e clonagem de VMs do cluster. Na Figura 1 irá apresentar os componentes que compõem a arquitetura da abordagem proposta.

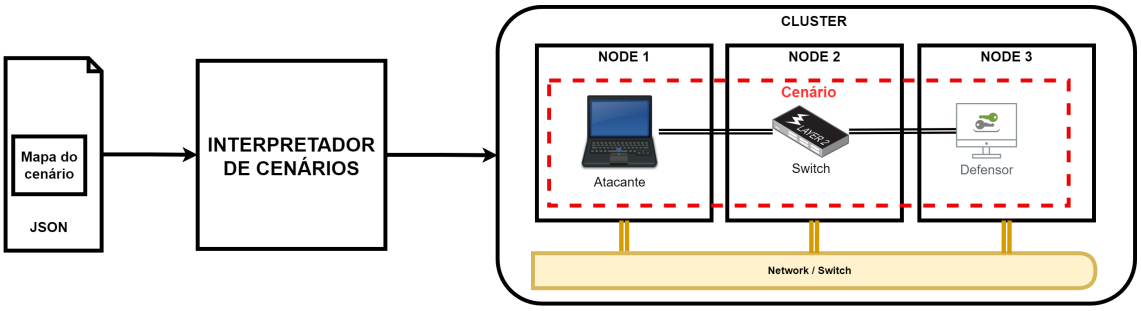


Figura 1. Abordagem para construção de cenários de ataque cibernético, baseada em *CyberRange* hospedado por cluster de alta disponibilidade.

O interpretador poderá baixar imagens de instalação de SO diretamente da internet, criar novas VMs e iniciar o processo de instalação, conforme as especificações de hardware; ou ainda poderá baixar modelos de VMs, diretamente da internet e implantá-los no cenário definido. Ele também será capaz de balancear o ambiente subindo os cenários de forma otimizada para o cluster, fazendo assim o melhor uso dos recursos disponíveis

Os *cenários* consistem na representação abstrata de uma rede real, com o objetivo de retratar ativos e passivos de uma rede específica. Essa representação pode ser criada pelo aluno ou disponibilizada pelo professor, permitindo que o aluno realize as atividades propostas no contexto da rede simulada e lide com diversas situações de forma prática. Ao imergir nesse cenário, os alunos podem explorar de maneira controlada e educativa os desafios e as dinâmicas que ocorrem em uma rede, possibilitando uma compreensão mais profunda dos princípios da segurança cibernética. Nesta proposta, um cenário poderá implementar os seguintes ativos e passivos:

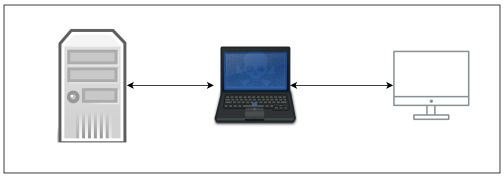
- **Servidor:** é um sistema computacional dedicado a fornecer recursos e serviços específicos para uma rede, atuando na camada 7 do modelo ISO/OSI.
- **Desktop:** é um sistema computacional completo, para simular um computador pessoal de uso comercial ou doméstico na rede, atuando na camada 7 do modelo ISO/OSI.
- **Switch:** é um ativo de rede que atua na camada 2 do modelo ISO/OSI, responsável por interconectar os membros da rede simulada.
- **Roteador:** é um ativo de rede que atua na camada 3 do modelo ISO/OSI, responsável pelo encaminhamento de pacotes de dados entre a rede simulada e a rede real. Serve como limitador do domínio de *broadcast* e impede a saída de tráfego malicioso do cenário da rede simulada.

3.1. Resultados Esperados

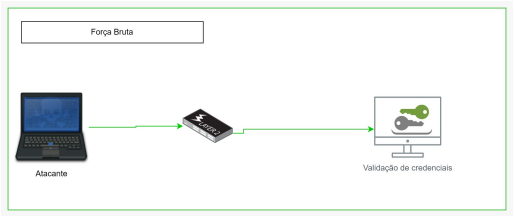
Espera-se que a abordagem proposta proporcione uma melhoria no processo de aprendizado e no desenvolvimento de habilidades dos alunos em SSI. Através da criação de ambientes virtualizados que simulem sistemas operacionais, redes e ativos de diferentes

camadas do modelo ISO/OSI, os estudantes terão a oportunidade de vivenciar situações reais e praticar técnicas e estratégias de SSI.

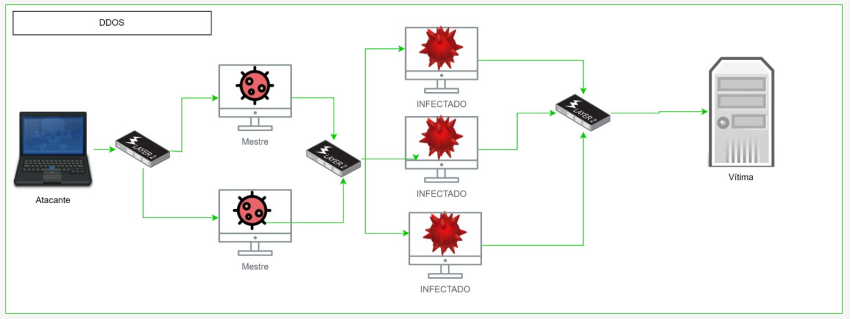
Abaixo são descritos três possíveis cenários, utilizando os ativos previstos: a Figura 2a apresenta um cenário de um ataque do homem-no-meio, composto por um servidor e dois desktops, nele podem ser apresentadas as vantagens da comunicação criptografada entre cliente e servidor; a Figura 2b apresenta um cenário de um ataque de força bruta, composto por um dois desktops e um switch, onde podem ser apresentadas estratégias de uso de firewall em estações de trabalho; por fim, a Figura 2c apresenta um cenário de ataque de negação de serviço, composto por vários desktops, três switchs e um servidor, onde podem ser apresentadas estratégias para mitigação de ataques de negação de serviço.



(a) Ataque do homem-no-meio.



(b) Ataque de força bruta.



(c) Ataque de Negação de Serviço.

Figura 2. Possíveis cenários de ataque cibernético para o ensino de Segurança de Sistemas de Informação.

4. Discussão

Este trabalho apresenta uma pesquisa em andamento que propõe do uso de CyberRange [Pham et al. 2016] hospedado em um cluster de alta disponibilidade para contribuir com o ensino de SSI através da abordagem baseada em casos [da Silva Melo and Oliveira 2020], contornando as dificuldades de instituições educacionais em aplicar conhecimentos práticos em SSI, devido à falta de recursos de processamento e memória em seus ambientes físicos.

Estão previstas pesquisas com docentes da área de SSI, sobre a infraestrutura computacional disponível em suas aulas, além de um questionário de aceitação de tecnologia, para avaliar as potencialidades da adoção desta proposta em atividades práticas de SSI.

Com base na experiência adquirida no período de pandemia, com a utilização de um cluster de alta disponibilidade no Laboratório de Redes, Desenvolvimento e

Segurança[5] do Cefet/RJ UnED Nova Friburgo, a prova de conceito deste trabalho utilizará o Proxmox, que se mostrou satisfatória para o atendimento das disciplinas da área de redes. O cluster é composto por 10 computadores desktops com a seguinte configuração: 1 Socket (4x Intel Core i5-3470 CPU), 32GB de memória RAM (4x 8GB DIMM DDR3-1600) e 3 discos (HDD 7200RPM - SATA - 500GB).

Referências

Bressan, G., Luis Gutiérrez López, F., Frota Redigolo, F., Nogueira Barbosa, A., Melo Silveira, R., and Vicente Ruggiero, W. (2022). VIRTUALIZAÇÃO DE EXPERIMENTOS DO LABORATÓRIO DIDÁTICO DE REDES DE COMPUTADORES PARA A FLEXIBILIDADE, REDUÇÃO DE CUSTOS E USO REMOTO. In *Proceedings of the L Brasilian Congress of Engineering Education*. Associação Brasileira de Educação em Engenharia. https://doi.org/10.37702/COBENGE.2022.4106.

Costa, P. V., Gonçalves, W. I., Gonçalves, E. D., and Lazarin, N. M. (2018). Nível de conhecimento de desenvolvedores sobre segurança em aplicações web: Pesquisa e análise. In *Anais da V Escola Regional de Sistemas de Informação do Rio de Janeiro*, pages 92–99, Porto Alegre, RS, Brasil. SBC. https://doi.org/10.5753/ersirj.2018.4661.

Cristani, M., Alves, W., Pereira, G., and Lazarin, N. M. (2020). Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no brasil. In *Anais Estendidos do XVI Simpósio Brasileiro de Sistemas de Informação*, pages 1–4, Porto Alegre, RS, Brasil. SBC. https://doi.org/10.5753/sbsi.2020.13114.

da Silva Melo, W. and Oliveira, F. K. d. (2020). Abordagens de ensino para segurança da informação: Possibilidades nos cursos online abertos e massivos. *Educação Profissional e Tecnológica em Revista*, 4(1):71–83. https://doi.org/10.36524/profept.v4i1.487.

Dantas, A. R. P. (2022). *CyRM: cyber range para auxiliar o ensino de defesa para alunos da disciplina de segurança da informação*. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores), Universidade Federal do Ceará, Quixadá. https://repositorio.ufc.br/handle/riufc/68364.

Pereira, G. d. S. (2019). *Firewall GNU/linux e IP tables: um estudo de implementação de ensino no plano de disciplina da formação do oficial de carreira de comunicações*. Trabalho de Conclusão de Curso (Bacharel em Ciências Militares) - Curso de Comunicações, Academia Militar das Agulhas Negras, Resende. https://bdex.eb.mil.br/jspui/handle/123456789/5590.

Pham, C., Tang, D., Chinen, K.-i., and Beuran, R. (2016). Cyris: A cyber range instantiation system for facilitating security training. In *Proceedings of the 7th Symposium on Information and Communication Technology*, SoICT '16, page 251–258, New York, NY, USA. Association for Computing Machinery. https://doi.org/10.1145/3011077.3011087.

Proxmox GmbH (2023). Proxmox - powerful open-source server solutions. https://www.proxmox.com/.

[5] https://pnipe.mctic.gov.br/laboratory/11002