Lab Cyber Academy: Um Cyber Range para Treinamento em Segurança da Informação Utilizando AWS e IaC

Vitor Reiel M. Lima[1], **Antonio Rafael P. Dantas**[2], **Michel S. Bonfim**[1,2], **João Marcelo U. Alencar**[2]

[1]Programa de Pós-Graduação em Computação (PCOMP)
Universidade Federal do Ceará (UFC) - Quixadá, CE - Brasil
[2]Universidade Federal do Ceará (UFC)
Av. José de Freitas Queiroz, 5003, 63902-580 – Quixadá, CE - Brasil

{vitorreiel, rafaelpinheiro.380}@alu.ufc.br
{michelsb, joao.marcelo}@ufc.br

Abstract. *Cybersecurity is essential due to the rapid evolution of cyber threats, which jeopardize the integrity of data and systems. Cyber Range are controlled virtual environments that allow the simulation of attacks (such as DDoS and vulnerability exploits) and defenses (such as firewalls and traffic analysis), promoting hands-on learning of security strategies. The Information Security discipline is fundamental in Information and Communication Technology courses, but the lack of free Cyber Ranges and resources in institutions hinders proper training. This work proposes the Lab Cyber Academy, a free Cyber Range solution that uses Containernet and Docker to create emulated attack and defense scenarios, implemented in the AWS Academy cloud and based on infrastructure as code. Experiments and evaluations with students from UFC prove its effectiveness, validating its feasibility for cybersecurity training.*

Resumo. *A segurança cibernética é essencial devido à rápida evolução das cyber threats, que colocam em risco a integridade de dados e sistemas. Cyber Range são ambientes virtuais controlados que permitem simular ataques (como DDoS e explorações de vulnerabilidades) e defesas (como firewalls e análise de tráfego), promovendo o aprendizado prático de estratégias de segurança. A disciplina de Segurança da Informação é fundamental nos cursos de Tecnologia da Informação e Comunicação, mas a falta de Cyber Ranges gratuitos e recursos nas instituições dificultam treinamentos adequados. Este trabalho propõe o Lab Cyber Academy, uma solução gratuita de Cyber Range que usa Containernet e Docker para criar cenários emulados de ataque e defesa, sendo implementada na nuvem da AWS Academy e baseada em infraestrutura como código. Experimentos e avaliações com alunos da UFC comprovam sua eficiência, validando sua viabilidade para treinamentos em cibersegurança.*

1. INTRODUÇÃO

A constante evolução das tecnologias da informação tem proporcionado avanços significativos em diversas áreas, melhorando a eficiência, a conectividade e a inovação [Urbach et al. 2018]. No entanto, essas transformações também trazem consigo desafios

consideráveis, especialmente no que diz respeito à segurança das informações. O aumento das ameaças cibernéticas fez com que a cibersegurança se tornasse um campo indispensável, exigindo atenção e recursos adequados para proteger dados sensíveis e sistemas críticos [Khan et al. 2022].

Segundo informações divulgadas pela *Fortinet*[1], um dos fatores que ocasionaram um aumento exorbitante de violações é pela grande escassez de profissionais com habilidades em cibersegurança no mercado [Maddison 2023]. Segundo [Costa et al. 2018], a falta de preparação adequada afeta diretamente a implementação de técnicas preventivas contra ataques cibernéticos. Uma maneira de suprir a carência de profissionais especializados em segurança da informação é através do incentivo e acompanhamento intensivo de treinamentos focados na área, que simulem cenários reais de ciberataques. Dessa forma, plataformas *Cyber Range* têm sido utilizadas.

De acordo com [Pham et al. 2016], o *Cyber Range* consiste em uma ferramenta voltada ao treinamento de cibersegurança. Essa ferramenta é capaz de criar ambientes virtualizados e controlados para a simulação ou emulação de cenários reais de ataques cibernéticos, e podem acompanhar exercícios práticos tanto de ataque (*e.g., Red team*) quanto de defesa (*e.g., Blue team*). Existem diferentes soluções de *Cyber Range*, desenvolvidas tanto pela academia como pela indústria. Em sua grande maioria são aplicações proprietárias com custos elevados e que consomem muito processamento e memória, o que as tornam inviáveis para implantação em ambientes acadêmicos, que geralmente possuem recursos computacionais limitados de *hardware*.

Nesse sentido, este trabalho propõe o **Lab Cyber Academy (LCA)**[2], uma solução gratuita de *Cyber Range* que utiliza *containers* para criar um ambiente emulado leve e eficiente. Utilizando a *AWS Academy*, o LCA oferece cenários de treinamento para capacitar estudantes, aproveitando a agilidade, flexibilidade e escalabilidade das soluções em nuvem. Além disso, adotando o conceito de Infraestrutura como Código (IaC), a infraestrutura na nuvem é provisionada e implantada automaticamente, garantindo eficiência e consistência. Foram implantados dois cenários de treinamento: um para o *Red team* e outro para o *Blue team*. Neste cenário, para orientar o processo de aprendizado, roteiros de estudo foram implementados no *Moodle*[3]. Finalmente, realizamos experimentos para avaliar o tempo de implementação na nuvem e o consumo de CPU e memória RAM nos laboratórios.

O restante deste trabalho está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A proposta é descrita na Seção 3. Finalmente, a Seção 4 conclui o artigo e apresenta trabalhos futuros.

2. TRABALHOS RELACIONADOS

O treinamento em ambientes controlados é essencial na cibersegurança para aprimorar habilidades de detecção e resposta a ameaças. Estudos destacam a relevância e complexidade do *Cyber Range*, explorando suas potencialidades e desafios.

Os autores [Pham et al. 2016] desenvolveram o *CyRIS*, um ambiente virtual-

[1]https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases
[2]https://github.com/vitorreiel/lab-cyber-academy
[3]https://moodle.org/?lang=pt_br

izado com *Kernel-based Virtual Machine* (KVM) e *CyTrONE*, enfocando a simulação de ataques estáticos e dinâmicos para identificação de vulnerabilidades, com destaque para a automatização de tarefas, embora a complexidade na configuração inicial seja um ponto fraco. Enquanto [Beuran et al. 2022] exploram a implementação do *CyRIS* na nuvem *AWS Elastic Compute Cloud (EC2)*, visando soluções escaláveis e de baixo custo para treinamentos em larga escala e evidenciam os desafios na configuração desse cenário. Os autores [Javali and Revadigar 2019] ressaltam a necessidade de validar ferramentas de segurança e propõem uma solução baseada em modelos estatísticos e uma *Graphical User Interface* (GUI) interativa, oferecendo geração de tráfego web realista para cenários de *Cyber Range*.

No trabalho de [Karjalainen and Kokkonen 2020], foi proposto um modelo conceitual de *Cyber Arena*, focado em ambientes de treinamento cibernético realistas e de larga escala, com capacidade de simular a internet e cenários organizacionais, além de permitir a avaliação de desempenho dos alunos. [Antonioli et al. 2017] abordaram a segurança dos Sistemas de Controle Industrial (ICS) através de treinamentos em *Capture The Flag* (CTF), divididos em fases online e ao vivo, com ênfase em competições gamificadas para profissionais e acadêmicos. Por outro lado, o artigo de [Nespoli et al. 2024] apresentou o *SCORPION*, um *Cyber Range* virtualizado com recursos de gamificação e análise de aprendizagem, incluindo monitoramento biométrico e ferramentas de criação de cenários flexíveis, mas sem suporte a equipes *red/blue*.

Os autores [Hatzivasilis et al. 2021] descrevem o *THREAT-ARREST*, uma plataforma avançada de treinamento cibernético que integra emulação, simulação, jogos sérios e visualização, utilizando modelos de ataques, cenários editáveis e agentes autônomos com comportamentos variáveis para capacitar usuários na resposta a ataques cibernéticos, oferecendo *logs* detalhados das sessões de treinamento, embora não seja *open-source*. Em contrapartida, [Lee et al. 2022] apresentam o *ICSTASY*, desenvolvido pela Agência Coreana para Desenvolvimento de Defesa, focado em treinamento cibernético militar, com cenários modelo, agentes autônomos, visibilidade dos instrutores, avaliação automatizada pós-exercício e técnicas de ataque do *MITRE* para agentes da *Red Team*, além de não ser *open-source*.

O trabalho proposto se destaca por oferecer uma solução leve e gratuita voltada à capacitação prática em segurança cibernética, utilizando emulação de redes com *Containernet* para simular cenários realistas de ataque e defesa. Diferentemente das abordagens existentes, que muitas vezes apresentam custos elevados e dependem de ambientes físicos robustos, o LCA combina o uso de *containers Docker*, provisionamento automatizado de fácil replicação e uma interface acessível e flexível para se destacar entre as demais soluções. Além disso, a proposta se diferencia por permitir a implementação de novos ambientes *Cyber Range* além dos que já são integrados (*Red Team e Blue Team*), facilitando o uso educacional e experimental da plataforma em contextos acadêmicos e profissionais.

3. LAB CYBER ACADEMY

Nesta seção, é detalhado a arquitetura e funcionamento do ***Lab Cyber Academy***. Além disso, também é detalhado os laboratórios disponíveis e o roteiro de estudo usado como apoio durante o treinamento.

3.1. Arquitetura

Como ilustrado na Figura 1 a arquitetura é composta por cinco camadas que permitem a adição de novas tecnologias, cenários de *Cyber Ranges* ou ferramentas. Sendo elas:

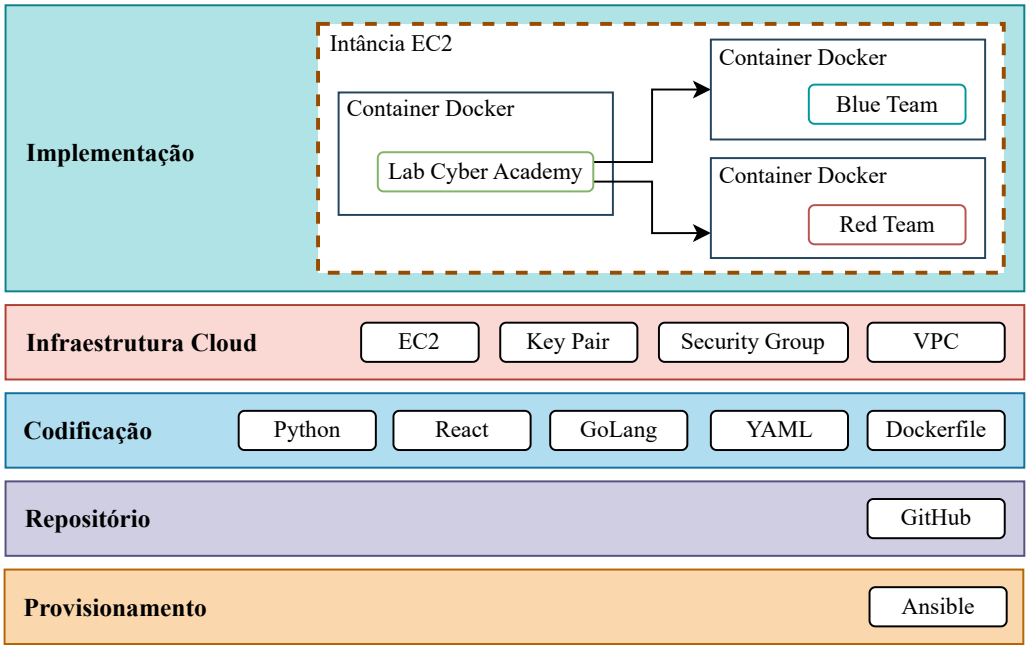

Figure 1. Arquitetura do LCA.

- **Implementação:** Esta camada contém os *containers Docker* da plataforma *Lab Cyber Academy*, gerados a partir de arquivos *Dockerfile* específicos para cada cenário. Os ambientes *Red team* (ataque) e *Blue team* (defesa) são acessados pelos alunos por meio da interface da plataforma, disponibilizada automaticamente ao final do provisionamento. Através dela, os usuários interagem com os componentes *Cyber Range* emulados pelo *Containernet* durante todo o treinamento.
- **Infraestrutura Cloud:** Nesta camada estão os componentes da infraestrutura do LCA. Durante o processo de provisionamento, é criada uma VPC juntamente com seus componentes (*Subnet, Route Tables, Gateway, Security Group, Key Pair*), seguida da criação de uma instância EC2 do tipo *t2.large*, com o *Ubuntu Server* 22.04 LTS e a liberação de portas de acesso, como 22 (SSH) e 9000 (LCA).
- **Codificação:** Essa camada inclui o código-fonte da plataforma, *scripts* e os *Dockerfiles* para criação dos *containers*, além dos arquivos de configuração dos *playbooks Ansible*, escritos em YAML. Sendo esta uma proposta *open source*, ela pode ser modificada e novos recursos podem ser implementados, seguindo os comentários deixados no código-fonte, instruções de formatação e as documentações disponibilizadas no repositório do GitHub.
- **Repositório:** Esta camada armazena e versiona o código-fonte dos componentes mencionados na camada de codificação, bem como documentações, exemplos, vídeos e materiais de apoio.
- **Provisionamento:** Esta camada é responsável por executar de forma automatizada o processo de provisionamento da infraestrutura e configuração da ferramenta, por meio de *playbooks Ansible*, utilizando a metodologia IaC. Diante disso, são realizadas a instalação e a implantação das dependências do LCA na plataforma AWS Academy.

3.2. Execução

Inicialmente, é necessário estabelecer a comunicação com a *AWS Academy*. Para isso, é necessário que o usuário insira as credenciais de acesso disponíveis em "AWS Details" no arquivo de configuração "aws_cli_access". Com os parâmetros das credenciais preenchidos, basta que o usuário execute o *script* inicial "./playbook.sh". Em seguida, o usuário poderá escolher se deseja executar o provisionamento de um novo ambiente em sua *cloud* (Opção 1) ou destruir a infraestrutura que já tenha sido criada anteriormente (Opção 2). Após digitar e confirmar o valor no terminal, o processo será iniciado.

3.3. Principais Funções

Esta plataforma conta com uma interface gráfica disponível para acesso com o seguinte formato de URL: `http://<ip_instancia>:9000`, com o intuito de simplificar o aprendizado dos alunos no treinamento de cibersegurança com *Cyber Range*. O *front-end* da plataforma foi desenvolvido utilizando o *framework React*, enquanto seu *back-end* foi desenvolvido com *GoLang*. Na tela inicial da plataforma, conforme ilustrado na Figura 2, podemos selecionar qual será o laboratório executado. Até o momento, temos disponíveis o Laboratório 1 (*Blue team*) e o Laboratório 2 (*Red team*). Além disso, também é possível acessar, com mais detalhes, as informações do laboratório clicando no botão com o símbolo "?" de cada laboratório. Após a seleção, ao clicar no botão "Iniciar", uma tela de carregamento será exibida, indicando a criação do ambiente. Em segundo plano, um *script Python* é executado no momento da seleção, contendo todas as configurações necessárias para executar uma infraestrutura de rede emulada através de *containers Docker*[4] com *Containernet*[5] para a criação dos *nós*. Vale ressaltar que, ao utilizar as diferentes imagens disponíveis no repositório oficial do *Docker* (*Docker hub*[6]), temos a flexibilidade para a criação de diferentes cenários de treinamento.

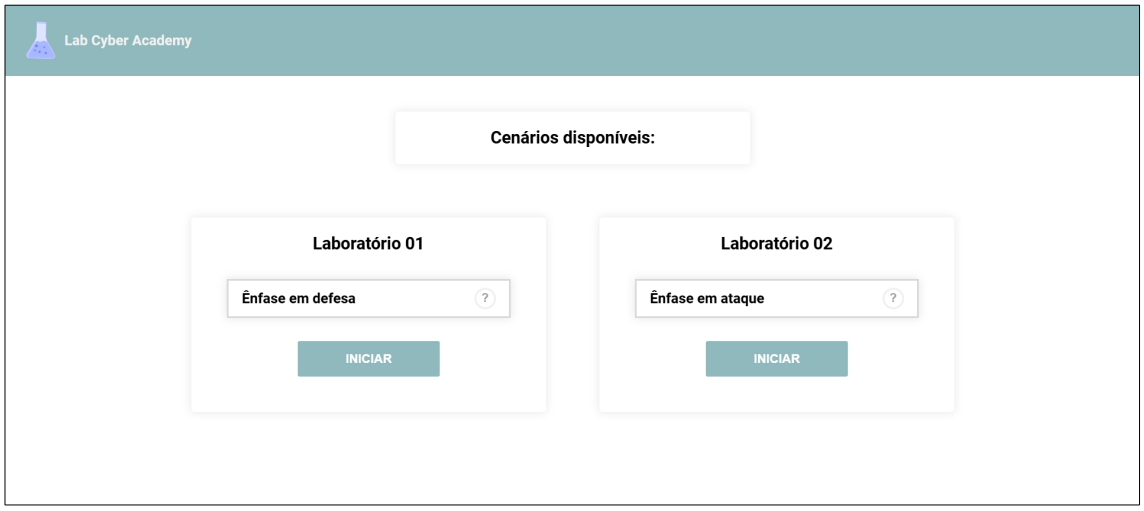

Figure 2. Tela Inicial do *Lab Cyber Academy*.

Após a finalização do processo de criação do laboratório, será automaticamente carregada uma interface semelhante à ilustrada na Figura 3 para o usuário. Essa será a in-

[4]https://www.docker.com/
[5]https://github.com/containernet/containernet
[6]https://hub.docker.com/

terface utilizada durante todo o treinamento, na qual os *nós* são representados por botões que podem ser selecionados com um simples clique. Esses *nós* são representações de componentes presentes em uma empresa fictícia que busca mitigar ataques cibernéticos recentes, sendo melhor detalhado na Seção 3.4. Cada seleção de *nó* gera destaque em seu botão. Além disso, ao lado, temos a CLI correspondente ao *nó* selecionado, que é automaticamente ajustada para cada nova seleção, assim o usuário poderá inserir comandos através da CLI de cada componente do cenário. Abaixo, uma imagem de exemplo do cenário *Blue team*:

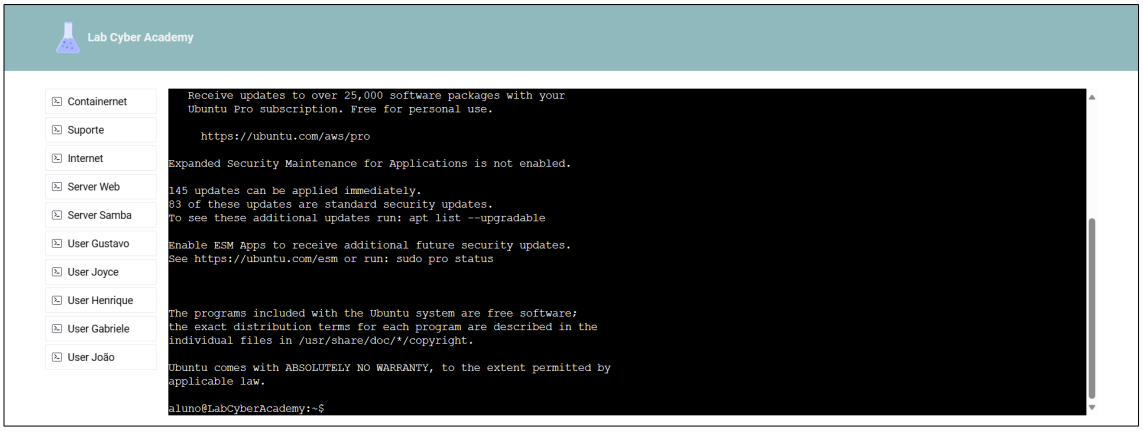

Figure 3. Tela de execução do cenário *Blue team*.

3.3.1. Definição do Cenário Blue team

Este cenário tem como objetivo simular a atuação de uma equipe de defesa cibernética dentro de uma rede corporativa, permitindo que os participantes desenvolvam habilidades na identificação, monitoramento e mitigação de ameaças. Para isso, os usuários interagem com a infraestrutura da rede emulada, analisam tráfego suspeito, verificam *logs* de eventos e aplicam medidas de proteção para reforçar a segurança do ambiente. Diante disso, utilizam ferramentas como *tshark*[7] para a análise de pacotes, configuram regras de *firewall* com *iptables* e enfrentam ataques simulados, incluindo *brute force* com *THC Hydra* e negação de serviço distribuído (DDoS). Além disso, a segmentação da rede em VLANs, como "DMZ 01" e "DMZ 02", permite testar estratégias de contenção e resposta a incidentes. Esse ambiente proporciona uma experiência prática para fortalecer mecanismos de defesa e preparar os alunos para desafios reais de segurança em redes corporativas.

3.3.2. Definição do cenário Red team

A topologia deste cenário é similar à do *Blue team*. No entanto, o objetivo aqui é explorar vulnerabilidades por meio de ataques manuais. Os alunos conduzirão ataques aos serviços *Samba* e SSH. No serviço *Samba*, o aluno utilizará a ferramenta *hping3* para realizar um ataque de negação de serviço, tornando o serviço indisponível. O outro ataque envolve um ataque de dicionário, onde o aluno usará a ferramenta *hydra* para verificar as credenciais.

[7]https://www.wireshark.org/docs/man-pages/tshark.html

No contêiner da Internet, o aluno deverá inicialmente criar as *wordlists* de login e senha. Em seguida, utilizando a ferramenta *hydra*, tentará descobrir as credenciais do servidor SSH. A ferramenta revelará o login e a senha do servidor e, se a descoberta for bem-sucedida, o aluno conseguirá se logar. O ataque será considerado bem-sucedido quando o aluno fornecer o login e a senha corretos como resposta.

3.4. Roteiro de Estudo

Para orientar o aprendizado dos alunos, foram criados questionários personalizados para cada laboratório, com cenários fictícios que abordando a detecção, diagnóstico e mitigação de ataques no ambiente de defesa (*Blue team*) e a indisponibilidade de acesso e descoberta de credenciais no ambiente de ataque (*Red team*). Diante disso, foram incluídas empresas fictícias que precisam mitigar tentativas de ataques cibernéticos ou executar ataques controlados em seus serviços para identificar possíveis vulnerabilidades. O usuário atuará como técnico em segurança dessas empresas e executará as atividades disponibilizadas. Esses questionários estão disponíveis nos formatos PDF e XML, compatíveis com a ferramenta *Moodle*. Embora a implantação do *Moodle* não seja parte deste trabalho, os usuários podem importar o questionário adequado à prática (defesa ou ataque) antes de utilizá-lo na plataforma *Lab Cyber Academy*. Na Figura 4, é apresentado um exemplo de atividade do cenário de defesa (*Blue team*) na interface do *Moodle*.

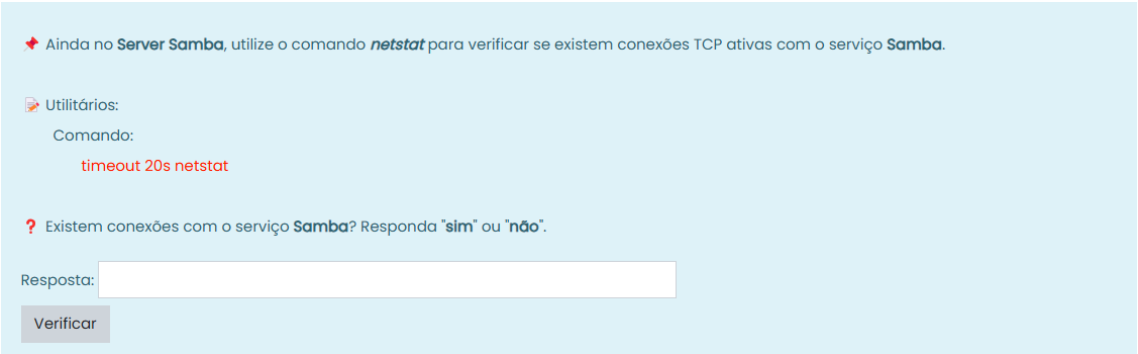

Figure 4. Questão exemplo do roteiro de estudo.

Repositório do código fonte: https://github.com/vitorreiel/lab-cyber-academy

Vídeo de instruções: https://acesse.one/lab-cyber-academy

4. CONCLUSÃO

Neste trabalho, identificamos a necessidade de uma plataforma de *Cyber Range* acessível às limitações das instituições de ensino. Propomos, assim, o *Lab Cyber Academy* (LCA), uma solução gratuita e com baixo consumo de recursos computacionais, baseada em um ambiente emulado e controlado com *containers* utilizando *Containernet* e *Docker*, permitindo a criação de cenários *Cyber Range* de ataque e defesa. Além disso, com o programa *AWS Academy*, foi possível executar os treinamentos na nuvem, tornando-os acessíveis aos estudantes. Para otimizar o processo, utilizamos métodos de *Infrastructure as Code* (IaC) para automatizar a criação da infraestrutura. Os *feedbacks* dos usuários foram essenciais para validar a viabilidade da plataforma, oferecendo uma perspectiva técnica sobre seu desempenho e usabilidade. Ao todo, obtemos 25 avaliações de alunos da

UFC, da disciplina de Segurança da Informação. Os resultados podem ser visualizados em gráficos de *Likert*, com notas de 1 a 5, sendo 1 a nota que indica o pior valor de qualidade e 5 a melhor. Esses gráficos podem ser conferidos ao final deste documento, em Anexos (Seção 5). Como trabalhos futuros, pretendemos aprimorar a escalabilidade do LCA, reduzir o tempo de implantação dos laboratórios, otimizar a experiência de navegação na interface da plataforma e explorar novas abordagens de *Cyber Range* para o desenvolvimento e integração de ambientes mais robustos e desafiadores.

References

Antonioli, D., Ghaeini, H. R., Adepu, S., Ochoa, M., and Tippenhauer, N. O. (2017). Gamifying ics security training and research: Design, implementation, and results of s3. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, CPS '17, page 93–102, New York, NY, USA. Association for Computing Machinery.

Beuran, R., Zhang, Z., and Tan, Y. (2022). Aws ec2 public cloud cyber range deployment. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 433–441.

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.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E. an d Koshutanski, H., Tsakirakis, G., Hildebrandt, T., Goeke, L., Pape, S., Blinder, O., Vinov, M., Leftheriotis, G., Kunc, M., Oikonomou, F., Magilo, G., Petrarolo, V., Chieti, A., and Bordianu, R. (2021). The threat-arrest cyber range platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 422–427.

Javali, C. and Revadigar, G. (2019). Network web traffic generator for cyber range exercises. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 308–315.

Karjalainen, M. and Kokkonen, T. (2020). Comprehensive cyber arena; the next generation cyber range. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 11–16. IEEE.

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., and Shin, J. (2022). Analyzing and evaluating critical cyber security challenges faced by vendor organizations in software development: Slr based approach. *IEEE Access*, 10:65044–65054.

Lee, D., Kim, D., Lee, C., Ahn, M. K., and Lee, W. (2022). Icstasy: An integrated cybersecurity training system for military personnel. *IEEE Access*, 10:62232–62246.

Maddison, J. (2023). Relatório anual da fortinet revela um aumento nas violações atribuídas à falta de habilidades em segurança cibernética.

Nespoli, P., Albaladejo-González, M., Valera, J. A. P., Ruipérez-Valiente, J. A., Garcia-Alfaro, J., and Mármol, F. G. (2024). Scorpion cyber range: Fully customizable cyberexercises, gamification and learning analytics to train cybersecurity competencies.

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.

Urbach, N., Ahlemann, F., Böhmann, T., Drews, P., Brenner, W., Schaudel, F., and Schütte, R. (2018). The impact of digitalization on the it department. *Business Information Systems Engineering*, 61.

5. Anexos

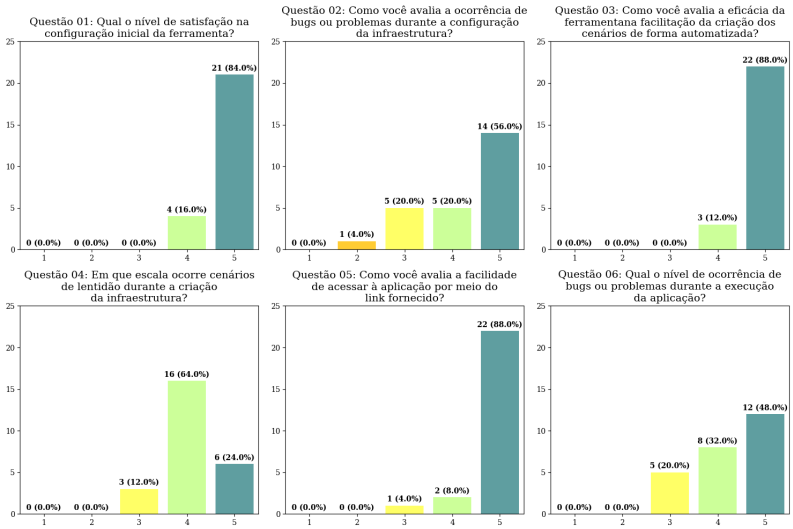

Figure 5. Resultados dos questionários de usabilidade da plataforma com alunos da UFC (Questões 1 a 6).

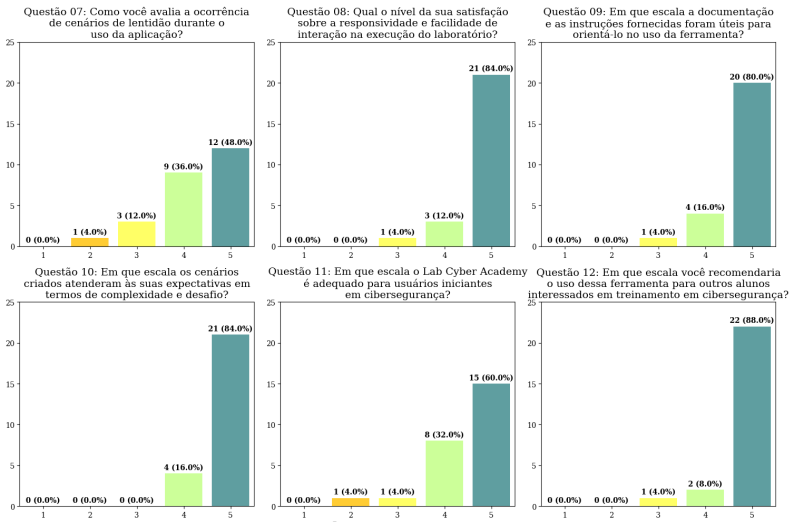

Figure 6. Resultados dos questionários de usabilidade da plataforma com alunos da UFC (Questões 7 a 12).