Dashboard HackInSDN: plataforma web para experimentação em redes e cibersegurança através de clusters Kubernetes

Italo Valcy S. Brito[1], **Leobino N. Sampaio**[1]

[1]Programa de Pós-Graduação em Ciência da Computação (PGCOMP)
Instituto de Computação – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

{italovalcy, leobino}@ufba.br

Abstract. *One way to address the quantity and complexity of cybersecurity incidents, which impact technological resources and sectors of society, is to invest in user awareness and advanced training for professionals with practical exercises and laboratories. Tools that simplify access to experimental environments with specialized networking and cybersecurity resources are essential in this context. This paper presents the HackInSDN Dashboard, a web platform that facilitates experimentation in networking and cybersecurity by orchestrating testbed resources. The Dashboard can be deployed to orchestrate resources from a Kubernetes cluster, enabling its use in cloud commercial environments and scientific testbeds, especially the Brazilian Research and Education Network (RNP) testbed. The tool has been used experimentally in undergraduate and graduate courses and proof-of-concept labs in the RNP's Hackers do Bem project.*

Resumo. *Uma das formas de lidar com a quantidade e complexidade dos incidentes de segurança, que impactam recursos tecnológicos e setores da sociedade, é investir na conscientização dos usuários e no treinamento avançado de profissionais, com exercícios práticos e laboratórios. Nesse sentido, ferramentas que simplifiquem o acesso a ambientes de experimentação com recursos especializados de redes e segurança são essenciais. Este artigo apresenta o Dashboard HackInSDN, uma plataforma web que facilita a experimentação em redes e cibersegurança a partir da orquestração de recursos de testbeds. O Dashboard pode ser implantado em ambientes Kubernetes, o que o habilita para uso em soluções comerciais de nuvem e diversos testbeds científicos, por exemplo, o Testbed da Rede Nacional de Ensino e Pesquisa (RNP). A ferramenta já vem sendo utilizada em caráter experimental em cursos de graduação, pós-graduação e turmas piloto no projeto Hackers do Bem da RNP.*

1. Introdução

Notícias recentes têm evidenciado incidentes de segurança de alto impacto global e com recordes históricos [Mirkovic et al. 2024]. Nesse cenário, treinamento, pesquisa e desenvolvimento em cibersegurança apresentam uma alternativa imprescindível para a salvaguarda das pessoas, infraestrutura e dados [Yamin et al. 2020]. Diversos ambientes de experimentação estão disponíveis [Gomez et al. 2023], tanto no contexto acadêmico quanto comercial. No geral, cada um deles possui um conjunto específico de recursos, características próprias e interfaces específicas de acesso, resultando em um desafio para

o usuário em aprender as APIs do ambiente e, muitas vezes, adaptar seus experimentos. Ademais, os diferentes ambientes de experimentação podem também impactar na repetibilidade dos experimentos entre diferentes instâncias – por exemplo, múltiplos alunos executando o mesmo laboratório –, além de reduzir a possibilidade de reuso e compartilhamento das receitas de laboratórios entre experimentadores. Uma interface comum que permitisse a abstração das APIs de cada *testbed*, tornando possível a federação dos ambientes e fornecendo um sistema em nuvem de Laboratório como serviço, tornaria esses ambientes mais acessíveis para serem usados em exercícios práticos de conscientização geral, capacitação em cibersegurança para profissionais, testes de qualidade e validação pré-produção, ou ainda experimentação para desenvolvimento de soluções de segurança.

Um sistema bastante comum nos ambientes de experimentação é o Kubernetes [Kubernetes 2025], uma plataforma de orquestração de contêineres e gerenciamento de recursos computacionais (processamento, rede, armazenamento, GPU, entre outros) bastante flexível, robusta e escalável, com ampla adoção em ambientes corporativos e ambientes de nuvem [Sfiligoi et al. 2024]. Como exemplo, a fundação de apoio à ciência nos Estados Unidos (NSF) tem financiado diversos projetos de implantação de Kubernetes [Sfiligoi et al. 2024] e, no Brasil, diversos projetos de experimentação em redes e cibersegurança seguem essa direção [Wangham et al. 2024], destacando-se o testbed da Rede Nacional de Ensino e Pesquisa (RNP) também conhecido como *Cluster Nacional* [Pedrosa et al. 2024], o testbed MENTORED que fornece um ambiente para pesquisa experimental em cibersegurança [Meyer et al. 2024], o projeto OpenRAN Brasil [Feferman et al. 2023] e o projeto BAMBU – Rede metropolitana para experimentação e inovação da Internet do Futuro em Salvador-Bahia [Sampaio 2025].

No geral, o Kubernetes é utilizado nesses projetos por facilitar a automatização da implantação, o dimensionamento e o gerenciamento dos recursos de experimentação. Por outro lado, embora o Kubernetes apresente ótimos mecanismos de orquestração, ele apresenta também uma curva de aprendizado íngreme [Malviya and Dwivedi 2022], o que pode se traduzir em maior tempo e esforço iniciais para uso do ambiente. No que tange ao uso desses ambientes para práticas de ensino, inclusive, a complexidade para começar a usar os recursos pode tirar o foco do objeto de ensino ou prática de laboratório, impactando as competências desenvolvidas [Santos et al. 2020].

Este artigo descreve a ferramenta Dashboard HackInSDN, uma plataforma web para execução de laboratórios virtuais baseada em um modelo de serviço em nuvem, que, na perspectiva do experimentador ou aluno, simplifica a execução dos laboratórios através de uma interface unificada, simples e escalável, e, na perspectiva do docente ou desenvolvedor do experimento, permite o reuso e compartilhamento das receitas de laboratório. O Dashboard HackInSDN abstrai a complexidade e especificidades dos principais ambientes de *testbed* disponíveis, além de agregar recursos específicos de segurança, oferecidos através da composição de software, para facilitar e ampliar o acesso aos recursos. Em particular, o Dashboard HackInSDN incorpora recursos da arquitetura HackInSDN[1] e foi implantado em fase piloto no *testbed* RNP (cluster Kubernetes). O Dashboard HackInSDN permite o desenvolvimento de laboratórios de cibersegurança em larga escala para treinamentos e experimentos, com rápida prototipagem, reuso de componentes e

[1]Grupo de trabalho do projeto Hackers do Bem para desenvolver uma arquitetura de suporte a experimentação e treinamento em redes e cibersegurança usando testbeds. `https://hackinsdn.ufba.br`

acesso a recursos de programabilidade de rede (e.g., switches P4). A execução do Dashboard HackInSDN requer apenas o acesso a um *namespace* de um cluster Kubernetes, o que viabiliza sua integração com ambientes existentes como o testbed RNP ou ainda permite o uso de servidores *bare metal* configurados com uma instância unitária do Kubernetes. Por fim, o Dashboard HackInSDN foi integrado com sistemas de autenticação federada que permitem o uso das credenciais da instituição de origem ou das redes sociais do usuário para acessar o sistema, o que, em conjunto com um modelo de autorização descentralizado, simplifica e flexibiliza a utilização do ambiente de experimentação.

A organização do artigo segue a seguinte estrutura: a Seção 2 apresenta a arquitetura, funcionalidades da ferramenta, casos de uso e disponibilidade de documentação; a Seção 3 descreve o planejamento da demonstração; por fim, a Seção 4 discute as considerações finais e os trabalhos futuros.

2. Dashboard HackInSDN

A Figura 1 ilustra de forma geral a arquitetura da ferramenta, e seus principais componentes serão descritos a seguir.

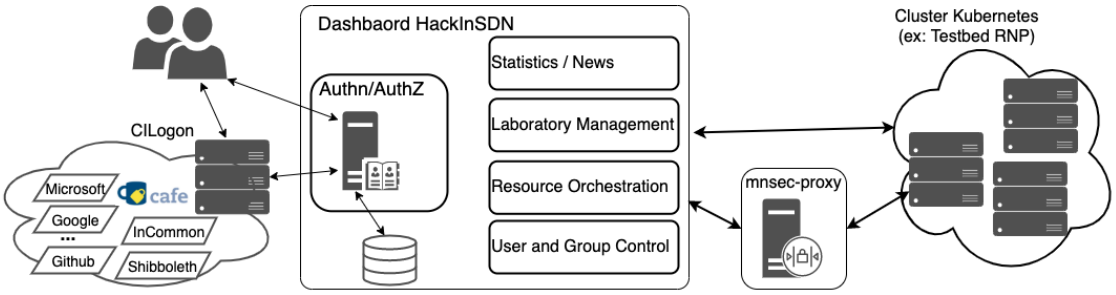

Figura 1. Arquitetura Dashboard HackInSDN.

Módulo de Autenticação (Authn/AuthZ). Este módulo encapsula o processo de autenticação na plataforma, que pode ocorrer de duas maneiras: autenticação local e autenticação federada através da plataforma CILogon[2]. Na autenticação local, o usuário cria suas credenciais no banco de dados local da aplicação. Na autenticação federada através do CILogon, o Dashboard HackInSDN lança mão do protocolo OAuth2 para consumir as APIs do CILogon, redireciona o usuário para o portal de autenticação do CILogon e, então, o usuário tem a possibilidade de escolher o Provedor de Identidade de sua preferência. Entre os provedores de identidade disponíveis, destacam-se as instituições pertencentes à Federação CAFe, mantida pela RNP. Assim, o Dashboard HackInSDN permite ao usuário valer-se das credenciais da sua instituição de origem no acesso ao sistema (i.e., credenciais dos sistemas acadêmicos e plataforma de EAD). Ademais, o CILogon também possui integração com diversos provedores de identidade de serviços como GitHub, Microsoft, Google, ORCID, entre outros, o que propicia o chamado "login social", onde o usuário faz uso de suas credenciais de redes sociais para acessar a plataforma. No primeiro acesso, o usuário é criado com perfil não privilegiado, e um administrador ou usuário com perfil de professor/experimentador precisa autorizar esse usuário para ter acesso aos recursos disponíveis no sistema.

[2]CILogon: Plataforma de gestão de identidade e acesso para ciência. `https://www.cilogon.org`

Módulo de Controle de Usuários e Grupos (*User and Group Control*). Após a aprovação do usuário, ele passa a ter acesso com um perfil de aluno e pode executar laboratórios de acordo com os grupos aos quais ele foi atribuído. O *Dashboard* permite a criação de grupos por professores e administradores a fim de facilitar a organização dos laboratórios e o controle de acesso. Cada usuário aprovado é automaticamente atribuído ao grupo "Todos" (*Everybody*), e o professor tem permissão para adicionar mais grupos ao usuário (individualmente ou em massa). O professor tem a possibilidade ainda de eleger membros do grupo como assistentes, delegando o controle de acesso a outros usuários (ex: monitores da disciplina). Por fim, o grupo possui também informações sobre data de expiração, período a partir do qual os recursos daquele grupo não mais estarão disponíveis (útil para cursos/experimentos que têm data de início e término bem definidos), e os grupos podem ser configurados com um *token* de acesso, que permite descentralizar o controle de membros do grupo.

Módulo de Estatísticas e Notícias (Statistics / News). O módulo de estatísticas é apresentado ao usuário na tela inicial do *dashboard* e funciona como um painel de atualizações e acompanhamento do estado do ambiente. É possível identificar a quantidade de laboratórios disponíveis, a quantidade de usuários, recursos disponíveis no ambiente de execução (CPU, memória, disco e pods), o mapa de nós que compõem o *cluster*, estatísticas de uso do ambiente e também os laboratórios recentemente adicionados. A página de estatísticas do *dashboard* apresenta ainda informações de *feedback* dos usuários e permite ao usuário enviar comentários, avaliar o ambiente e receber alertas de futuras manutenções, ações agendadas, laboratórios a finalizar em curto prazo, entre outras.

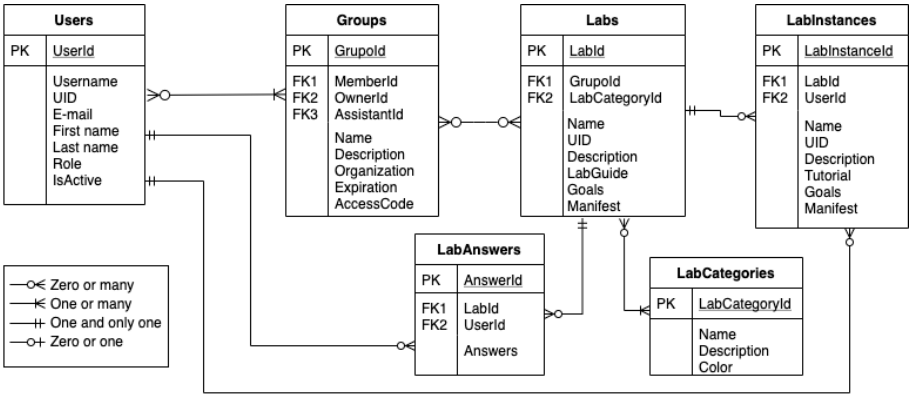

Figura 2. Diagrama Entidade-Relacionamento do Dashboard HackInSDN.

Módulo de Gestão de Laboratórios (*Laboratory Management*). A gestão de laboratórios é um processo central no Dashboard HackInSDN, pois eles são o principal objeto de consumo dos experimentadores, alunos e professores. Nesse sentido, foi criada uma modelagem de dados de forma a prover relacionamentos flexíveis e semanticamente significativos na plataforma. Em particular, a Figura 2 ilustra o modelo de entidade-relacionamento utilizado na construção da base de dados da plataforma. Em termos da modelagem para os laboratórios, é possível observar a entidade Laboratório (Lab) e Instância de Lab. Um lab pode ter múltiplas instâncias de execução, porém cada instância pode estar associada a um usuário e a um lab. Além disso, um usuário pode executar apenas uma instância do mesmo lab por vez, sendo permitido executar múltiplas instâncias desde que de diferentes labs. Cada lab possui informações sobre os *guias* de

execução associados, também conhecidos como roteiros de laboratório ou tutoriais, os quais descrevem os passos que o aluno deve seguir para realizar o experimento completo e atingir os *objetivos* estabelecidos para aquele laboratório em questão. O criador do laboratório pode definir ainda restrições do lab do tipo: quantidade máxima de CPU alocada, quantidade máxima de memória, quantidade máxima de tempo, quantidade máxima de Pods, imagens que podem ser utilizadas em cada Pod, nós nos quais as instâncias serão criadas, entre outras. Tais restrições são implantadas e reforçadas através do componente *mnsec-proxy*, que permite a criação dinâmica de Pods e links entre eles para formar a topologia de rede necessária para o Lab através do Mininet-Sec [Brito and Sampaio 2024]. O guia de laboratório, disponível após iniciá-lo, fornece não apenas um roteiro de atividade, mas também, de forma interativa, permite a inclusão de perguntas (texto livre, múltiplas escolhas, etc.) que, ao final, podem ajudar o professor a medir o desempenho ou engajamento do aluno. Por fim, a instância de execução dos labs possui um atributo de agendamento, onde o executor especifica qual o período em que deseja executar aquele laboratório. A execução do lab pode ser estendida múltiplas vezes, e ao expirar, os recursos são liberados para outros experimentos.

Módulo de Orquestração de Recursos (*Resource Orchestration*). O módulo de orquestração de recursos foi criado a fim de facilitar a gestão de *Pods*, *Deployments*, *Services* e demais recursos disponíveis no cluster Kubernetes para os administradores do Dashboard. A partir desse módulo, o administrador possui uma visão global do ambiente e pode tomar ações de gerenciamento como remoção de *Pods*, checagem da saúde do sistema, reconfiguração de recursos, entre outras.

2.1. Interface do Dashbaord HackInSDN

O Dashboard HackInSDN provê uma interface web simples e flexível, que permite ao professor cadastrar laboratórios e disponibilizar guias de aprendizagem. Os alunos podem executar os laboratórios em qualquer lugar e horário, tendo como requisito apenas um navegador *web*. A Figura 3 ilustra duas telas da ferramenta: a figura mais interna com borda vermelha (número 1) apresenta a tela inicial da ferramenta, onde o usuário tem a visualização das estatísticas do ambiente, bem como notícias e informações gerais. Já a figura mais externa (com número 2) mostra uma visualização dos labs disponíveis para execução, conforme autorização do grupo. O usuário pode filtrar os labs pelas categorias, visualizar a descrição, vídeos e imagens para entender o que será abordado.

Uma vez que o usuário decida por executar um laboratório, ele poderá acompanhar a execução através da tela de Labs em Execução, conforme ilustrado na Figura 4. A Figura 4 possui três capturas de tela de diferentes abas que podem ser abertas ao interagir com o Dashboard: a) mais à direita da Figura 4 (quadrado com número 1), o usuário pode visualizar a tela principal da visualização do lab em execução, listando o título do Laboratório, o usuário que está executando o laboratório e os recursos instanciados para aquele laboratório: Pods, serviços, consoles de cada Pod e informações como endereço IP e status de execução. Em seguida, tem-se o guia de laboratório, onde, além do passo a passo para execução, o aluno pode copiar os comandos para executar nos hosts (evitando erros de digitação) e perguntas que o professor pode inserir ao longo do roteiro para avaliar o progresso/engajamento do aluno. Ainda na Figura 4 mais à esquerda (quadrado com número 2), pode-se observar uma aba que é aberta ao clicar no serviço "Mininet-Sec". Nessa tela, o usuário tem a visualização da topologia exata que compõe

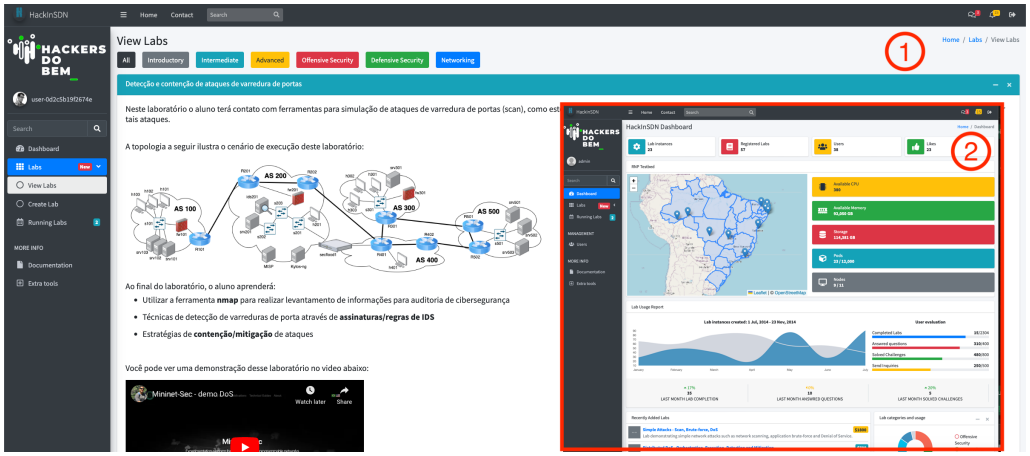

Figura 3. Visualização de Labs no Dashboard HackInSDN.

esse laboratório. A partir dessa topologia, o usuário pode visualizar os *links*, visualizar os *hosts*, executar comandos nos hosts e diversas outras funcionalidades presentes no Mininet-Sec [Brito and Sampaio 2024]. Por fim, na parte de baixo à direita da Figura 4 (quadrado com número 3) o usuário tem acesso a um console do Pod no navegador, para que possa interagir com o experimento de acordo com o roteiro de laboratório.

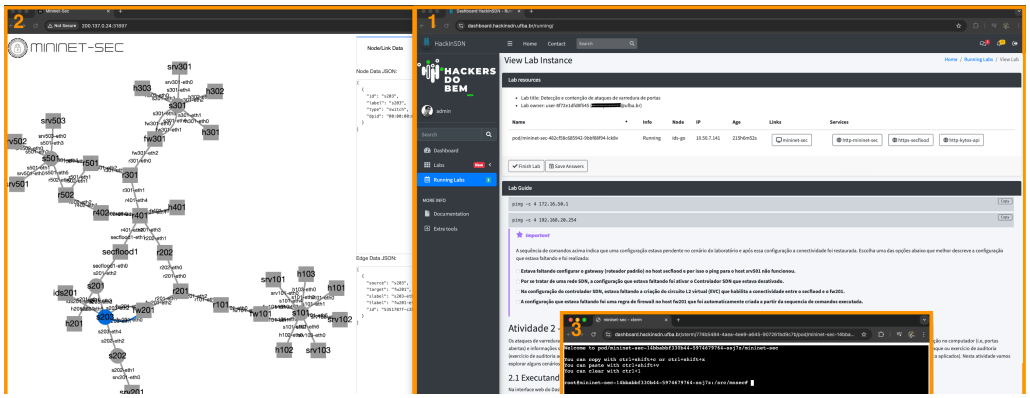

Figura 4. Labs em Execução no Dashboard HackInSDN.

Outro aspecto que merece destaque acerca do Dashboard é que ele apresenta-se como uma instância da arquitetura HackInSDN[3]. Portanto, além das funcionalidades e recursos específicos do Dashboard, ele incorpora integrações com outros componentes da arquitetura e possui exemplos de laboratórios com a composição destes componentes. O principal exemplo desta integração é o Mininet-Sec [Brito and Sampaio 2024], que inclusive motivou a inclusão de um módulo no Dashboard chamado "mnsec-proxy" (ver 1). O Mininet-Sec permite criar e gerenciar topologias diversificadas para os labs, integrando nós da topologia que são baseados em *namespaces de redes* do Linux e *Pods* do Kubernetes – conectados via túneis VXLAN, L2TP ou *sockets* UDP – o que permite criar experimentos de larga escala em termos de quantidade de nós. O Mininet-Sec incorpora ainda nós do tipo *switches* programáveis, roteadores, *firewalls*, IDS, *network taps*[4],

[3]Trabalho submetido para publicação. Site do projeto: `https://hackinsdn.ufba.br`

[4]Network TAPs são dispositivos de rede que permitem espelhamento de tráfego na camada física.

serviços de rede (e.g., DNS, HTTP, SMTP), e está em desenvolvimento a integração com switches P4 reais e outros tipos de nós. Outros componentes da arquitetura HackInSDN integrados ao Dashboard são: Secflood, sistema de geração de tráfego benigno e malicioso com diferentes perfis e volumetria; MISP, uma plataforma de compartilhamento de informações de Inteligência de Ameaças; Suricata e Zeek, sistemas de detecção de intrusão e monitoramento de segurança.

2.2. Manuais e documentação

O código-fonte do Dashboard HackInSDN, manuais de instalação e uso, informações de licenciamento, além de alguns vídeos explicativos sobre suas funcionalidades, podem ser encontrados no repositório do projeto, disponível em `https://github.com/hackinsdn/dashboard`. Além disso, o site do projeto HackInSDN também apresenta documentações sobre o Dashboard: `https://hackinsdn.ufba.br/tutoriais`

3. Planejamento de Demonstração

O Dashboard HackInSDN foi projetado para prover serviços de laboratórios virtuais em nuvem, tornando acessível a experimentação em ambientes de larga escala como o Testbed RNP. Dessa forma, a demonstração dar-se-á simplesmente com o suporte de uma televisão e um computador com acesso à Internet. A partir destes recursos, planeja-se demonstrar as principais funcionalidades da ferramenta, incluindo: autenticação federada; visualização de estatísticas sobre o ambiente de experimentação em uso; visualização de laboratórios; inicialização de um laboratório; acesso aos recursos do laboratório; interação com o laboratório a partir do roteiro e das perguntas disponíveis; encerramento do laboratório e liberação de recursos; processo de criação de novos laboratórios.

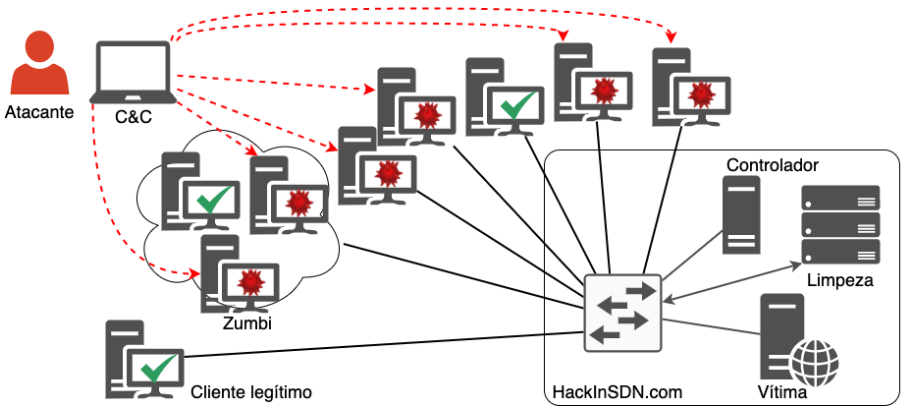

Figura 5. Topologia para o laboratório de DDoS.

Durante a demonstração será apresentado o **Laboratório de execução, detecção e mitigação de ataques de DDoS**[5]. Ataques de negação de serviço distribuídos (DDoS, do inglês *Distributed Denial-of-Service*) se caracterizam pelo volume de tráfego gerado e diversidade de origem, visando indisponibilizar um serviço ou seus componentes adjacentes [Aslam et al. 2022]. Na demonstração serão ilustrados os processos de execução, detecção e mitigação de ataques de DDoS utilizando o Dashboard HackInSDN, instanciando e orquestrando recursos no Testbed RNP. A Figura 5 apresenta o cenário utilizado

[5]`https://github.com/hackinsdn/labs/tree/main/lab04-ddos`

na demonstração. Neste cenário, considera-se algumas máquinas infectadas com vírus que funcionam como *bots* atacando um servidor web (vítima). Em paralelo, apresenta-se como um cliente legítimo observa os impactos do ataque a partir da indisponibilidade em acessar o servidor web. O ataque será identificado a partir do monitoramento *sFlow* e regras de bloqueio serão criadas no *switch* programável a partir do controlador SDN para conter o ataque, seja através do bloqueio simples ou através de um processo de limpeza de tráfego em equipamento especializado.

Além do laboratório supracitado, durante a demonstração serão apresentados outros laboratórios disponíveis na plataforma, a saber: Laboratório de *pentest* de aplicações web através de ataques de injeção de código SQL; Laboratório de varredura de rede, ataques de força bruta e de negação de serviço simples; tunelamento DNS; dentre outros.

4. Considerações finais e Trabalhos Futuros

Este artigo apresentou o Dashboard HackInSDN, uma plataforma web que facilita a experimentação em redes e cibersegurança a partir da orquestração de recursos de *testbeds* disponíveis, permitindo a criação de laboratórios que podem ser utilizados em larga escala por estudantes, profissionais e pesquisadores para executar os experimentos de forma simples, isolada e integrada. A ferramenta vem sendo utilizada em disciplinas de graduação e pós-graduação em fase piloto, bem como em uma prova de conceito com alunos do programa Hackers do Bem da RNP.

O Dashboard HackInSDN foi desenvolvido com suporte inicial para ambientes de experimentação baseados em Kubernetes, o que o habilita para os principais ambientes de nuvem comerciais, ambientes corporativos baseados em Kubernetes e ainda alguns dos principais ambientes de testbed científicos disponíveis, com destaque para o Testbed RNP. O uso do Kubernetes como plataforma de execução permite grande escalabilidade, isolamento e limitação de recursos, bem como elasticidade pela adição ou remoção de poder computacional ao cluster. É possível também executar a ferramenta em ambientes locais, seja com uma máquina virtual ou servidor dedicado, sendo suficiente instalar o Kubernetes (e.g., instalação em único nó) e executar uma instância do Dashboard. Ou ainda, utilizar a ferramenta integrada com múltiplos testbeds simultaneamente.

O Dashboard HackInSDN está em contínua evolução e trabalhos futuros incluem: otimizações na plataforma para aprimorar o suporte a práticas de ensino de redes e segurança utilizando *testbeds* (e.g., recursos de usabilidade, novos laboratórios); integração com outros ambientes de experimentação, a exemplo do testbed FABRIC[6]; e integração com componentes físicos, como switches programáveis P4, nos quais utilizaremos uma API de orquestração remota destes nós baseada em gNOI/gNNI e substituição do pipeline P4 implantado no sistema operacional (ex: no SONIC, RARE, OpenNetworkLinux ou qualquer outro sistema que permita carregamento de um pipeline P4 customizado, tal qual aqueles supracitados).

Agradecimentos

Os autores agradecem o apoio da Rede Nacional de Ensino e Pesquisa (RNP), do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB).

[6]`https://portal.fabric-testbed.net`

Referências

Aslam, N., Srivastava, S., and Gore, M. M. (2022). ONOS Flood Defender: An Intelligent Approach to Mitigate DDoS Attack in SDN.

Brito, I. V. S. and Sampaio, L. N. (2024). Mininet-sec: plataforma de experimentação para segurança cibernética em redes programáveis. *Salão de Ferramentas - SBRC*.

Feferman, D. L., Hernandez, M. P., Santos, W. M., Chagas, M. S., Araújo, G. H., Oliveira, L. B., and Lima, G. C. (2023). Orquestração multidomínio no testbed openran@ brasil. In *Workshop de Testbeds*, pages 62–73. SBC.

Gomez, J., Kfoury, E. F., Crichigno, J., and Srivastava, G. (2023). A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, 237:110054.

Kubernetes (2025). Kubernetes. `https://kubernetes.io`. Accessed: 2025-01-10.

Malviya, A. and Dwivedi, R. K. (2022). A comparative analysis of container orchestration tools in cloud computing. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 698–703.

Meyer, B. H., Gemmer, D. D., de Santana, K. G., Ferreira, J. V., de Mello, E. R., Nogueira, M., and Wangham, M. S. (2024). Criação e análise de datasets de ataque de negação de serviço usando o mentored testbed. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 812–825. SBC.

Mirkovic, J., Kocoloski, B., and Balenson, D. (2024). Enabling reproducibility through the sphere research infrastructure. *login Usenix Mag.*

Pedrosa, E., Martins, J., Sousa, F., Mondin, L., and Dias, G. (2024). Indo além das simulações com o serviço de testbeds: Ambientes reais para experimentação científica em tics. In *Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF)*, pages 47–54. SBC.

Sampaio, L. (2025). Bambu: Uma plataforma de inovação metropolitana para promover pesquisa sobre a internet do futuro na cidade de salvador. `http://insert.ufba.br/projetos-bambu/`. Accessed: 2025-01-10.

Santos, J. B., Ribeiro, A. V., Brito, I. V. S., de Souza, M. C. S., de Souza Matos, E., and Sampaio, L. N. (2020). Uma experiência de avaliação multidimensional de cursos de redes de computadores em ambientes de testbeds. In *Anais do XXXI Simpósio Brasileiro de Informática na Educação*, pages 1703–1712. SBC.

Sfiligoi, I., Würthwein, F., Dost, J., Lin, B., and Schultz, D. (2024). Demand-driven provisioning of kubernetes-like resources in osg. In *EPJ Web of Conferences*, volume 295, page 07014. EDP Sciences.

Wangham, M. S., Meyer, B. H., Gemmer, D. D., de Santana, K. G., Frank, L. R., de Campos, L. E. F., de Mello, E. R., and Schwarz, M. F. (2024). Testbeds para pesquisa experimental em cibersegurança: Da teoria à prática. *Minicursos do Simpósio Brasileiro de Redes de Computadores - SBRC*.

Yamin, M. M., Katt, B., and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636.