



GT-HackInSDN

Infraestrutura programável em testbed para ensino de redes e segurança

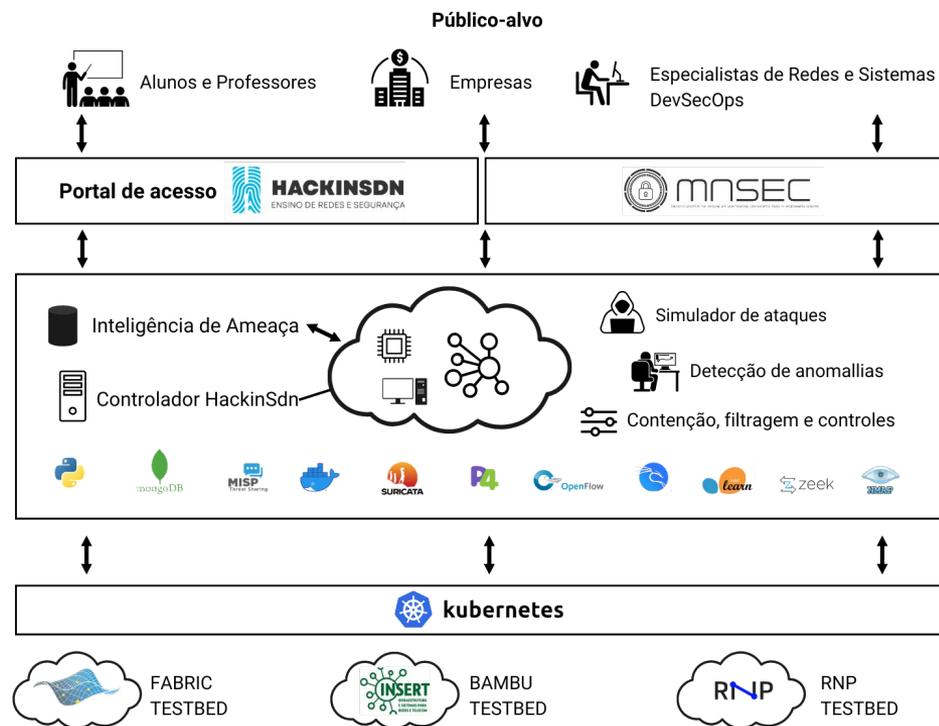
Leobino Sampaio

Universidade Federal da Bahia (UFBA)

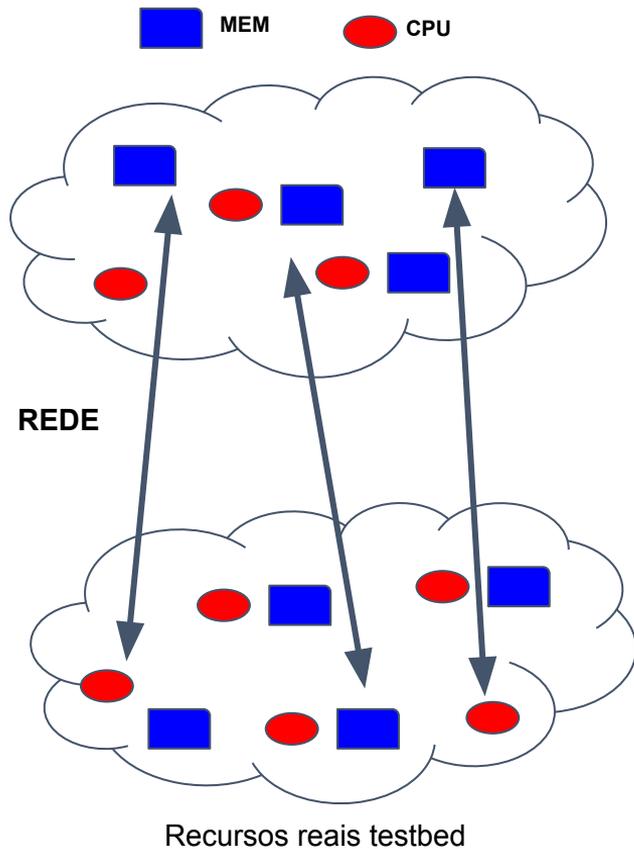
O que é a HackInSDN?



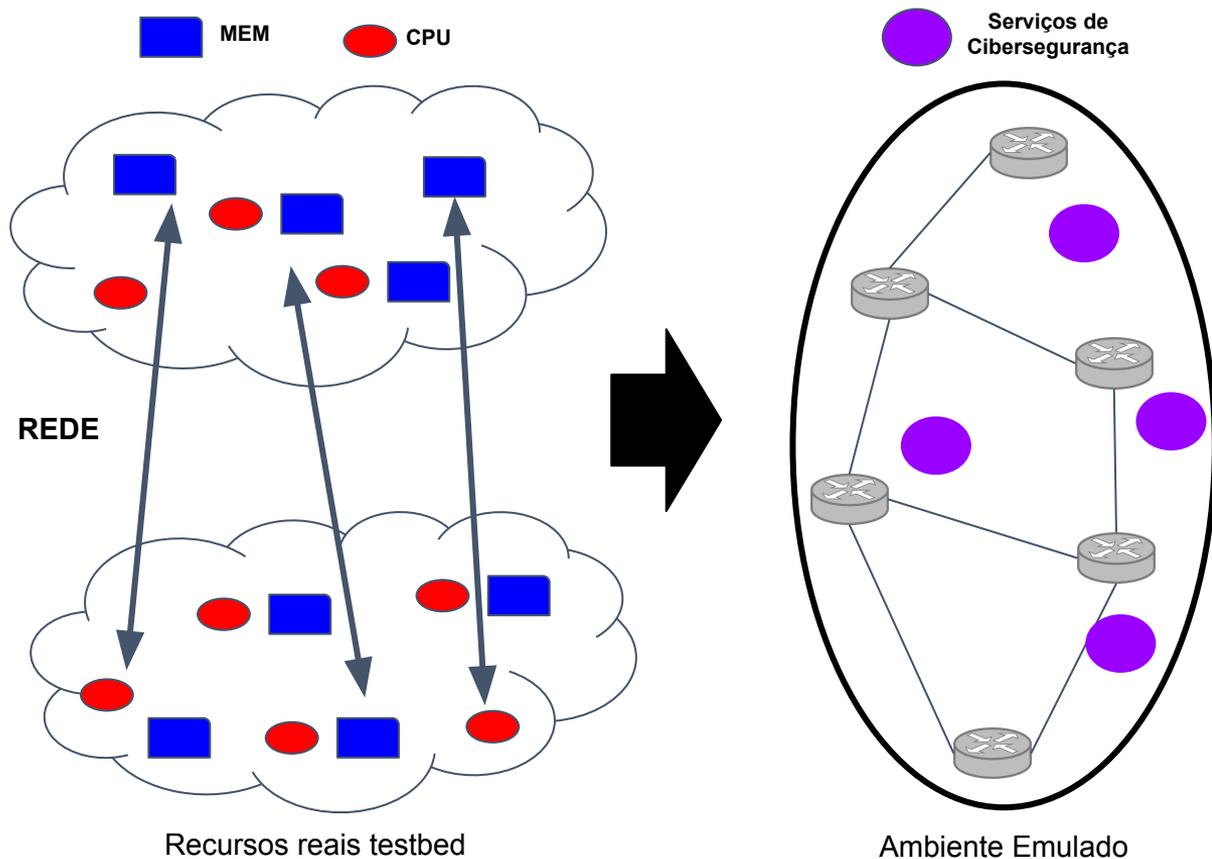
Um ambiente que provê recursos computacionais **reais** e **distribuídos** e **serviços** para apoiar a capacitação em cibersegurança



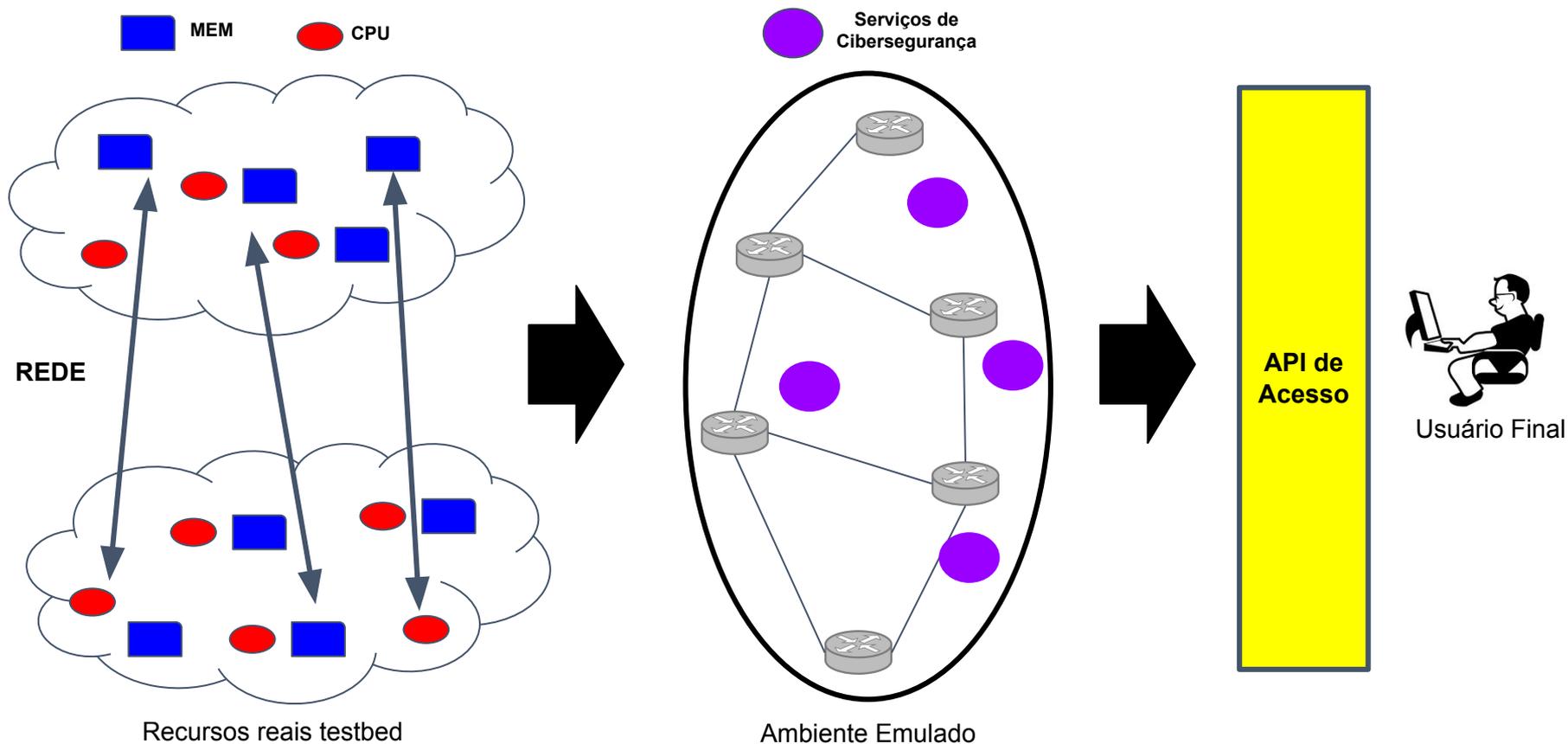
Componentes reais e distribuídos



Serviços de cibersegurança

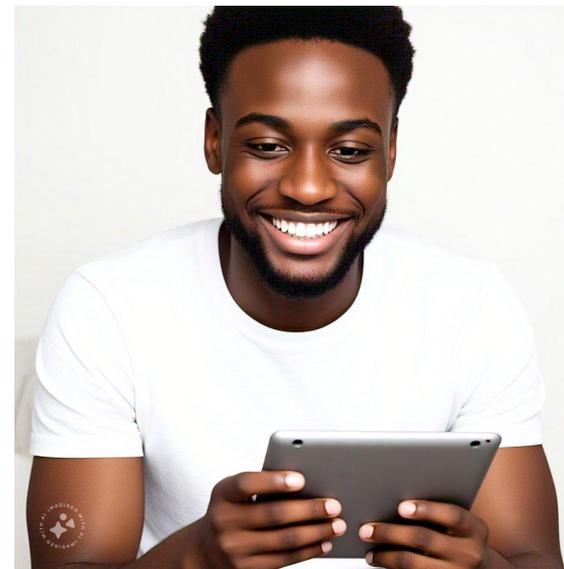


Abstração para usuário final



Principais benefícios

- Recursos computacionais reais
 - Cenários de capacitação mais realistas
 - Maior disponibilidade de recursos que implica em menor restrição de experimentação
- Distribuição
 - Reuso e otimização de recursos computacionais
 - Capacitação em rede, formação de equipes de diferentes localidades
- Serviço oferecido em nuvem (**LabaaS**)
 - Escalabilidade
 - Facilidade de acesso (web)

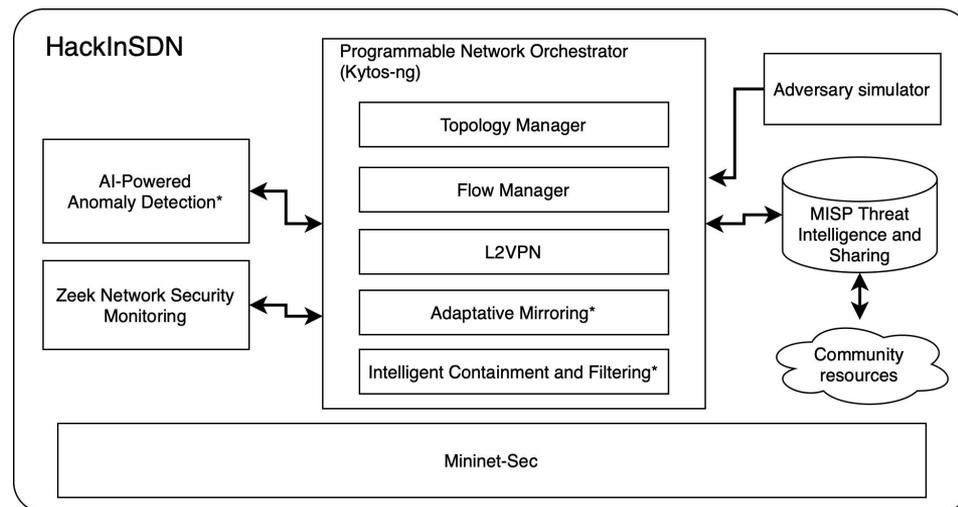


Como os objetivos foram alcançados?

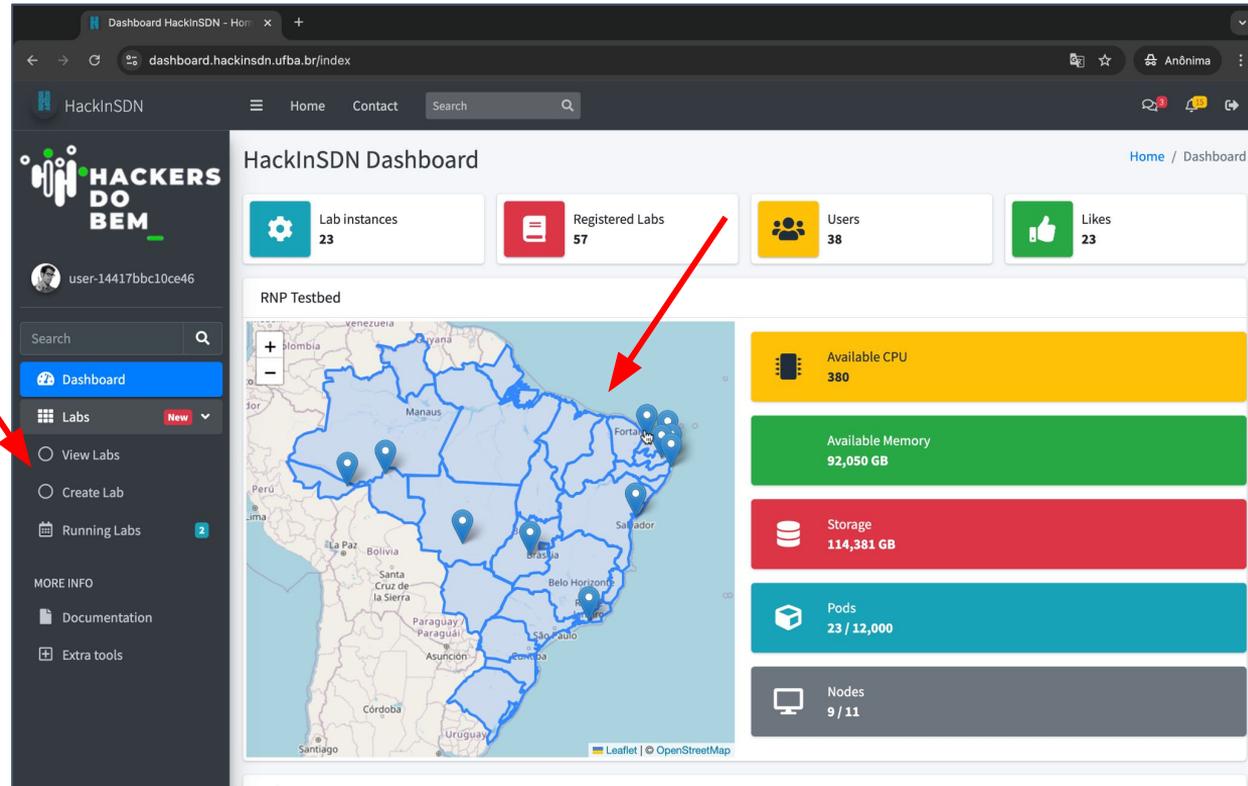
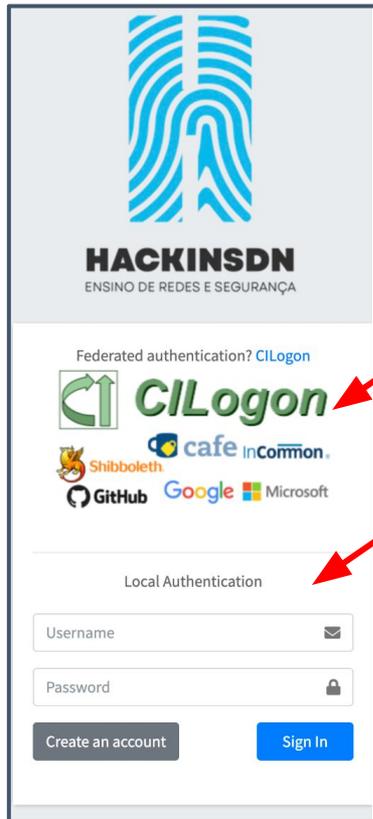
- Objetivo geral
 - Desenvolvimento de uma Infraestrutura programável em testbed para ensino de redes e segurança
- Características
 - Redes Definidas por Software (SDN)
 - Baixo acoplamento dos módulos
 - Desenvolvimento baseado no uso de contêineres de código aberto
 - Adoção de componentes de software já existentes
 - Integração ao serviço de testbeds da RNP
 - Desenvolvimento de um portal de acesso



kubernetes



Funcionamento da plataforma



The image shows the HackInSDN Dashboard. The top navigation bar includes "Home", "Contact", and a search bar. The main content area features several widgets: "Lab instances" (23), "Registered Labs" (57), "Users" (38), and "Likes" (23). Below these is a map titled "RNP Testbed" showing various locations in South America. A red arrow points to the map. To the right of the map are four status bars: "Available CPU" (380), "Available Memory" (92,050 GB), "Storage" (114,381 GB), and "Pods" (23 / 12,000). At the bottom right, there is a "Nodes" section showing 9 / 11. A red arrow points to the "Registered Labs" widget. The left sidebar contains a search bar, navigation links for "Dashboard", "Labs", "View Labs", "Create Lab", "Running Labs", "Documentation", and "Extra tools".

Uso da plataforma

- Caso de uso
 - Detecção de ataques de varredura, força bruta e negação de serviço
- Elaboração de roteiros de ensino
- Alinhamento com projeto e plano de ensino de cursos de computação
- Capacitação experimental
 - Membros do grupo de pesquisa não envolvidos no projeto
 - Disciplina graduação curso de computação da UFBA
 - Auditoria e Segurança de Sistemas

The image displays two screenshots of the Mininet-Sec platform interface. The top screenshot shows a meeting titled "Sala de Encontro" at 14:35, with a participant named "Italo Valcy da Silva B...". The interface includes a sidebar with "MENSAGENS", "Perguntas", "Bate-papo público", "NOTAS", and "USUÁRIOS (26)". The main area shows a network graph and a table of statistics:

Parameters	Latencies	Bytes	Status Codes	Others
Targets: http://172.16.50.1	P50: 2.292768ms	Total: 103650	*500: 50	I: 5.102217
Rate: 5	P90: 2.934175ms	Mean: 2073		Rate: 0.000000
Duration: 10s	P95: 3.289335ms	Out: 0		Success: 0.000000
Method: GET	P99: 8.107658ms	Total: 0		Earliest: 2024-11-22T00:32:17Z
	Max: 8.107658ms	Mean: 0		Latest: 2024-11-22T00:32:17Z
	Min: 1.403185ms			Mod: 2024-11-22T00:32:17Z

The bottom screenshot shows a meeting titled "Sala de Encontro" at 14:35, with a participant named "Maysara Rodrigues E...". The interface includes a sidebar with "MENSAGENS", "Perguntas", "Bate-papo público", "NOTAS", and "USUÁRIOS (23)". The main area shows a network graph and a terminal window displaying the output of a Mininet-Sec scan:

```
443/tcp open  https
nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
root@minsec:~# nmap -sS 172.16.50.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-22 00:12 UTC
Nmap scan report for 172.16.50.1
Host is up (0.0005s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@minsec:~# nmap -sS 80.443.172.16.50.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-22 00:12 UTC
Nmap scan report for 172.16.50.1
Host is up (0.0005s latency).
All 1000 scanned ports on 172.16.50.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
root@minsec:~# nmap -sS 172.16.50.1
```

Atuação da equipe



- SBSeg 2024 - S.J. dos Campos
- Reunião CT-Cibesegurança ITA-SP
- Workshop de testbeds WTR PoP-Ba
- HackBahia 2024
- EnSI 2024
- Workshop MISP do CERT.br 2024
- VII Conferência Tecnologia e Infância MP-Ba
- Reuniões de grupo de trabalho

Anais Estendidos do SBSeg 2024: SF



Mininet-Sec: plataforma de experimentação para segurança cibernética em redes programáveis

Italo Valcy S. Brito¹, Leobino N. Sampaio¹

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

{italovalcy, leobino}@ufba.br

Abstract. *This paper presents Mininet-Sec, an emulation platform for studying and experimenting with cybersecurity in programmable networks. Mininet-Sec allows rapid prototyping of cybersecurity scenarios, attack simulation, and testing offensive security tools in an isolated and secure environment. The availability of specialized resources, along with support for network programmability, enables fast, effective and skilled development of security solutions. Mininet-Sec will be demonstrated in a variety of scenarios, including secure interdomain routing, DDoS attacks, and network security teaching, revealing how one can leverage Mininet-Sec's resources to provide advanced cybersecurity labs.*

Resumo. *Este artigo apresenta o Mininet-Sec, uma plataforma de experimentação de cibersegurança em redes programáveis, que permite rápida prototipagem de cenários de segurança, simulação de ataques e testes de ferramentas de segurança ofensiva de forma isolada. A disponibilidade de componentes específicos de segurança somado à capacidade de programabilidade da rede permitem o desenvolvimento rápido, eficaz e especializado de soluções de segurança. A ferramenta será demonstrada em cenários diversificados incluindo roteamento inter-domínio seguro, ataques de DDoS e práticas de ensino de segurança de redes, mostrando como os recursos do Mininet-Sec podem ser com-*

Atuação da equipe



Equipe

- **Coordenação acadêmico**
 - Leobino Sampaio (UFBA)
- **Coordenador assistente**
 - Italo Valcy (FIU)
- **Pesquisadores**
 - Allan Edgard (IFBA)
- **Bolsistas**
 - Talita Pinheiro (Doutoranda UFBA)
 - Gustavo Santos (Mestrando IFBA)
 - Henrique Scoppetta Sampaio (Graduando UFBA)
 - Mayara Rodrigues (Graduanda UFBA)
 - Raquel Santos (Graduanda UFBA)



Obrigado!



leobino@ufba.br



Vamos para a Demo ?

<https://dashboard.hackinsdn.ufba.br>