PAINEL – Segurança Cibernética na Era da IA: Desafios e Oportunidades?

GUSTAVO Neves DIAS | *Gerente de Serviços*
Diretoria de Pesquisa, Desenvolvimento e Inovação - DPDI
Rede Nacional de Ensino e Pesquisa - RNP

RNP

Educação, Pesquisa
e Inovação em Rede

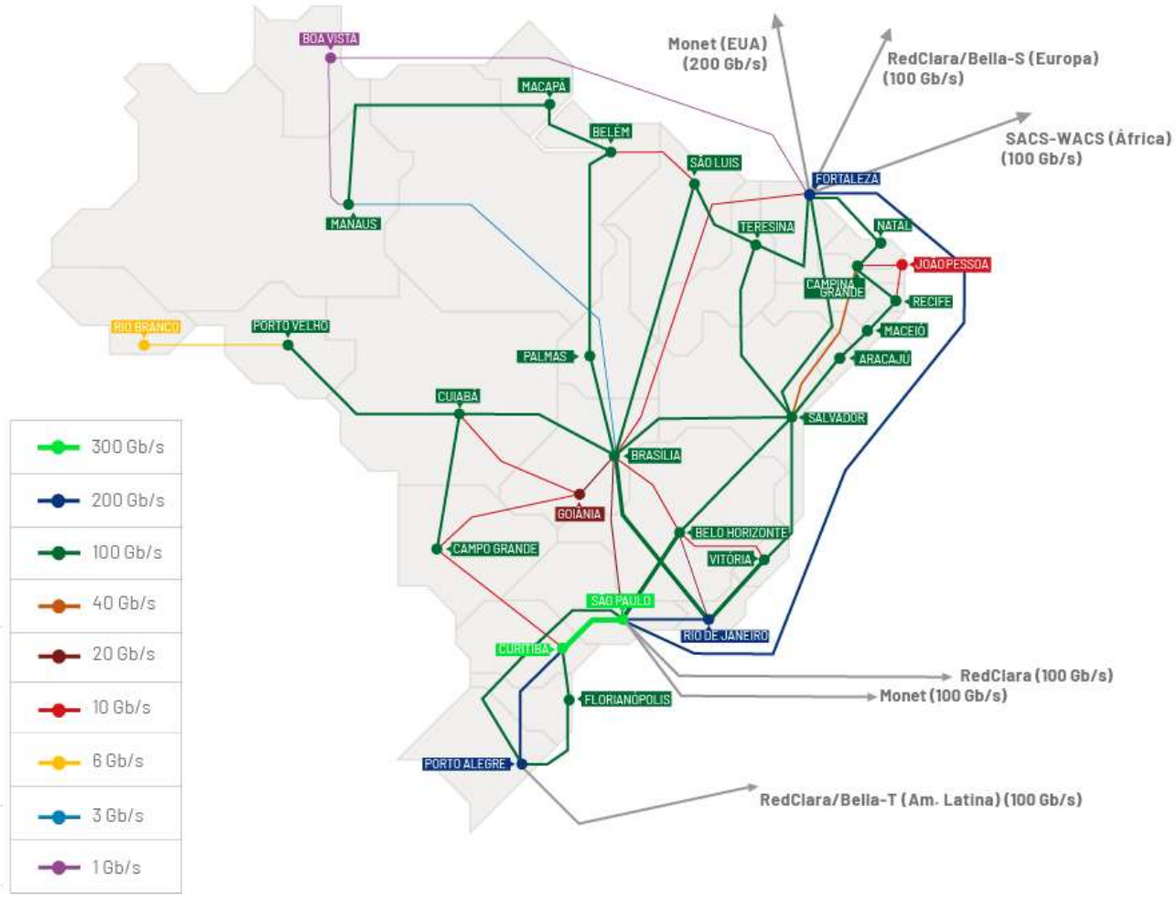
9ª Escola Regional de Informática do Espírito Santo
ERI-ES 2024 - 19/10/2024

ERIES Escola Regional de Informática ES

QUEM AQUI CONHECE A RNP ?

Rede Nacional de Ensino e Pesquisa

A RNP conecta as instituições de *ENSINO, PESQUISA E INOVAÇÃO* do Brasil em uma rede e liga essa comunidade com o mundo.



Nossa **REDE ACADÊMICA** está em todo o território nacional, interiorizando oportunidades e ***beneficiando mais de 3 milhões de alunos, professores e pesquisadores.***

Rede Nacional de Ensino e Pesquisa

Disponibilizamos *Serviços Seguros*...

ConferênciaWeb
FileSender@RNP
eduplay
Diploma Digital
ICPEdu
INFRAESTRUTURA DE CHAVES PÚBLICAS PARA ENSINO E PESQUISA
ICPEdu
CERTIFICADO PESSOAL
fone rnp
eduroam
cafe
comunidade acadêmica federada
TEST BEDS
RNP
CAIS
nas nuvens

Rede Nacional de Ensino e Pesquisa

E junto com ALUNOS, PROFESSORES E PESQUISADORES, desenvolvemos novas tecnologias com foco em inovação contínua.

PD&I em CIBERSEGURANÇA

PROGRAMA Hackers do Bem

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

- RNP em parceria com o SENAI-SP e a Softex

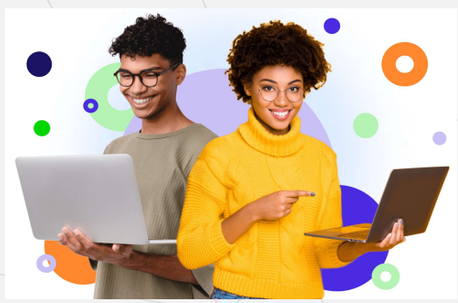
3 Principais PILARES

HACKERS DO BEM

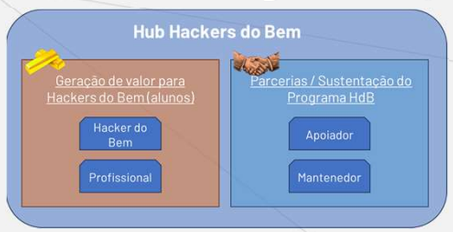
hackersdobem.org.br

- Nivelamento
- Básico
- Fundamental
- Especializado
- Residência Tecnológica

Capacitação



HUB Nacional de Cibersegurança



https://hub.hackersdobem.org.br/

PD&I em Cibersegurança

Aberta chamada para seleção de projetos de P&D em Cibersegurança

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

Capacitação – Grandes números

HACKERS DO BEM

- Nivelamento
- Básico
- Fundamental
- Especializado
- Residência Tecnológica

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

HUB Nacional de Cibersegurança

https://hub.hackersdobem.org.br/

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

Programa de P&D em Cibersegurança

HACKERS DO BEM

Editais de Financiamento de Projetos de P&D

1º ciclo de P&D	Inicial 12 meses	Extensão 6 meses	2023 e 2024
2º ciclo de P&D	Inicial 12 meses	Extensão 6 meses	2024 e 2025

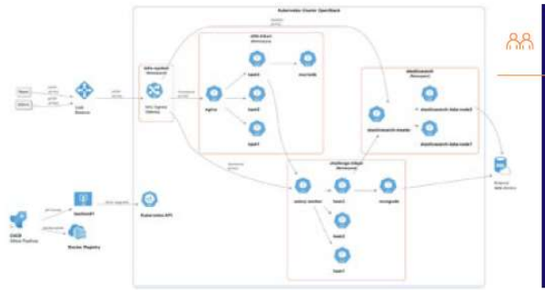
Segunda Chamada de P&D Lançada em 05 de Agosto de 2024

(Eixos Temáticos definidos como resultado do I Workshop sobre Formação em cibersegurança)

https://www.rnp.br/inovacao/editais

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

ITA



FICHA TÉCNICA

COORDENADOR- GERAL/ ACADÊMICO: Lourenço Alves Pereira Júnior – Instituto Tecnológico de Aeronáutica (ITA), ljr@ita.br

EQUIPE: Sidnei Barbieri, Caio Marcos Chaves Viana e Leonardo Gonçalves Chahud

HIKARI
Hunting Integrado

PLATAFORMA DE COMPETIÇÃO ONLINE EM DEFESA CIBERNÉTICA E CAÇA DE AMEAÇAS

COMPETIÇÃO E APRENDIZADO EM RESPOSTA A INCIDENTES

A crescente complexidade das ameaças cibernéticas demanda ferramentas de treinamento eficazes para equipes de defesa, destacando a importância de ambientes práticos para o aprimoramento de habilidades em análise forense, compreensão de logs e desenvolvimento de estratégias contra técnicas de atacantes. Nesse contexto, propõe-se a criação de uma plataforma online que simule redes reais para treinamento em defesa cibernética, enfocando habilidades de investigação de incidentes e caça a ameaças cibernéticas.

Tal plataforma replicará o ambiente de um Centro de Operações de Segurança (SOC), usando ferramentas de código aberto, como ELK, e Kubernetes isolados para cada equipe, com uma infraestrutura central baseada em Elasticsearch. Serão apresentados desafios baseados em cenários hipotéticos, orientados por questionários, com sistema de pontuação para avaliar a capacidade de resposta a incidentes. O projeto pretende desenvolver competências técnicas, trabalho em equipe e análise crítica.

Ao mimetizar desafios do mundo real em um ambiente controlado, o projeto visa a preencher uma lacuna na educação em cibersegurança, capacitando profissionais para responder eficientemente a ameaças emergentes. Esse ambiente simulado promove um aprendizado profundo das dinâmicas de segurança cibernética, essencial para equipes de defesa modernas.

UFF

Os módulos do emulador de ataques XSS

Um emulador educativo de **ataques de cross-site scripting (XSS)**

GT-EXSS

O GT-EXSS propõe um emulador de ataques Cross-Site Scripting (XSS) para o aprendizado prático em cibersegurança. No XSS, um atacante explora vulnerabilidades de sites legítimos para executar trechos de código maliciosos nos navegadores dos usuários legítimos. As vulnerabilidades exploradas por atacantes são encontradas em campos de sites que permitem a entrada de dados pelos usuários legítimos e retornam informações sobre os dados de entrada para esses usuários. Mais de 60% dos sites têm algum tipo de vulnerabilidade XSS.

O emulador permite que usuários identifiquem sites vulneráveis a ataques XSS em um ambiente controlado. Isso se dá através de atividades compostas por uma introdução teórica sobre o assunto, seguida de procedimentos

Revista do WRNP 2024

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

UFMG

Priorização contextualizada de vulnerabilidades **orientada a negócio**

MAXIMIZANDO O IMPACTO DE EQUIPES DE SEGURANÇA

FICHA TÉCNICA

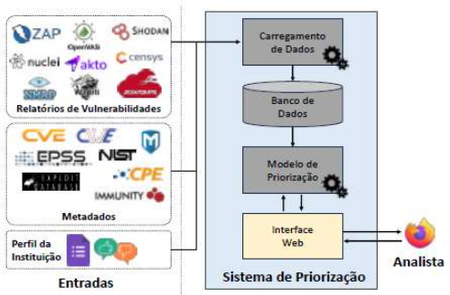
COORDENADOR-GERAL/ACADÊMICO: Ítalo Cunha - Universidade Federal de Minas Gerais (UFMG), *cunha@dcc.ufmg.br*

EQUIPE: Francisco Teixeira Rocha Aragão, Gabriel Pains de Oliveira Cardoso, Lucas Santana do Carmo Sacramento e Pedro Henrique Meireles de Almeida

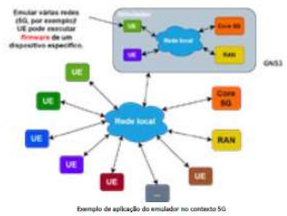
A comunidade de segurança identifica, cataloga e desenvolve ferramentas para detectar novas vulnerabilidades continuamente. Devido à complexidade, à dinamicidade e ao alto nível de integração de sistemas computacionais modernos, a execução dessas ferramentas identifica muitas fragilidades, frequentemente de severidade crítica. A alta taxa de vulnerabilidades identificadas sobrecarrega equipes de segurança, dificultando que organizações as investiguem e mitiguem em tempo hábil.

Neste projeto, desenvolveremos soluções para priorizar vulnerabilidades, considerando o contexto de cada organização. Por exemplo, uma empresa de análise de crédito pode priorizar aquelas que permitem vazamento de dados e afetam a privacidade de seus clientes, enquanto uma firma de distribuição de conteúdo pode priorizar outras que afetem o desempenho ou a disponibilidade do serviço.

Vulnerabilidades recentes, com provas de conceito, em sistemas críticos ou bibliotecas populares devem ser tratadas com prioridade, haja vista a elevada chance de serem alvo de ataques e causarem danos. Vamos construir um motor de priorização que combine múltiplas fontes de dados, incluindo o contexto e o perfil da organização, e refiná-lo iterativamente utilizando o feedback de analistas. Esperamos ganhos concretos de segurança direcionando esforços para que equipes consigam mitigar um número maior de vulnerabilidades mais relevantes.



UFCG



Exemplo de aplicação do emulador no contexto 5G.

FERRAMENTA FLEXÍVEL E DINÂMICA PARA FORMAÇÃO EM SEGURANÇA CIBERNÉTICA

Emulador para treinamento em **segurança cibernética**

ANÁLISES E TESTES DE SEGURANÇA

FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO: Edmar Candeia Gurjão - Universidade Federal de Campina Grande (UFCG), *ecg@dee.ufcg.edu.br*

EQUIPE: Leocarlos B. S. Lima, Matheus V. P. dos Santos, Ana Júlia Gouveia, Fernando Barros, João Paulo G. Barbosa e Luara Delai

O emulador é um ambiente de aprendizagem virtual que permite a interação com meios físicos, dedicado à análise e ao teste de segurança em redes de computadores e redes móveis (TI – Tecnologia da Informação) e Infraestruturas Críticas (TO – Tecnologia de Operação). Materializa a compreensão prática da avaliação de vulnerabilidades e ameaças, a realização de ataques e emprego de ferramentas para mitigação de riscos, bem como o conhecimento em áreas subjacentes.

O ambiente proposto oferece aos usuários, sejam eles aprendizes de segurança cibernética ou profissionais que desejam se aprimorar, uma abordagem orientada ao entendimento dos conceitos por meio de ações alinhadas às práticas convencionais adotadas por profissionais da área. Adicionalmente, propõe-se a criação de uma experiência progressiva de aprendizado gamificado, permitindo que os participantes testem e consolidem seus conhecimentos.

O ambiente fundamenta-se em uma arquitetura virtualizada, escalável e adaptável, que abarca desde o nível introdutório até o avançado no espectro de conhecimento na área de redes.

Atende às demandas atuais de formação e prática em segurança cibernética. Ao facultar a exploração tangível das técnicas e ferramentas críticas em um ambiente controlado, o projeto contribuirá significativamente para o aprimoramento dos estudantes e futuros profissionais no campo da segurança cibernética.

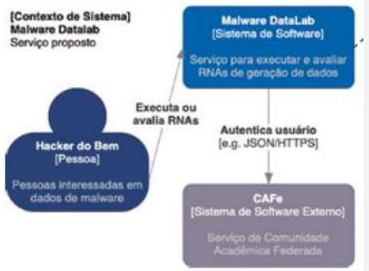
Revista do WRNP 2024

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

UNIPAMPA

Malware DataLab: inteligência artificial para detecção de malwares

DADOS SINTÉTICOS PARA QUALIFICAR SOLUÇÕES BASEADAS EM IA



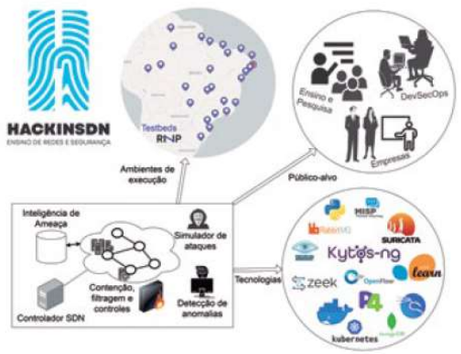
O nível da proliferação de malwares é alarmante devido ao fato de Hackers do Mal estarem empregando técnicas sofisticadas de Inteligência Artificial (IA). Para enfrentar esse desafio, é importante que Hackers do Bem compreendam e adotem abordagens de IA, como modelos preditivos acurados. No entanto, o sucesso desses modelos depende da qualidade e quantidade dos dados usados no seu treinamento.

O Malware DataLab surgiu com o propósito de disponibilizar um serviço para reduzir a curva de aprendizado e facilitar a investigação de técnicas avançadas de IA generativa para geração de dados úteis no treinamento de modelos de detecção de malwares. Como ponto de partida, o projeto vem desenvolvendo as ferramentas DroidAugmentor e AutoDroid. Enquanto a DroidAugmentor incorpora IA generativa através de Redes Neurais Artificiais (RNAs) e permite que o Hacker do Bem possa investigar de maneira sistemática técnicas atuais de IA generativa, a AutoDroid viabiliza a execução da DroidAugmentor de maneira escalável. Um dos desafios conhecidos da IA generativa está relacionado à capacidade computacional necessária para o treinamento dos modelos.

Como resultados do projeto, pretendemos disponibilizar novas versões das duas ferramentas e um serviço online, com interface gráfica, onde o Hacker do Bem vai ser capaz de experimentar, compreender e validar diferentes configurações de modelos de IA generativa na geração de dados sintéticos.

VIABILIZAR O USO DE TÉCNICAS DE IA GENERATIVA NA DETECÇÃO DE MALWARES

UFBA



Infraestrutura programável em testbed para ensino de redes e segurança

GT HACKINSDN

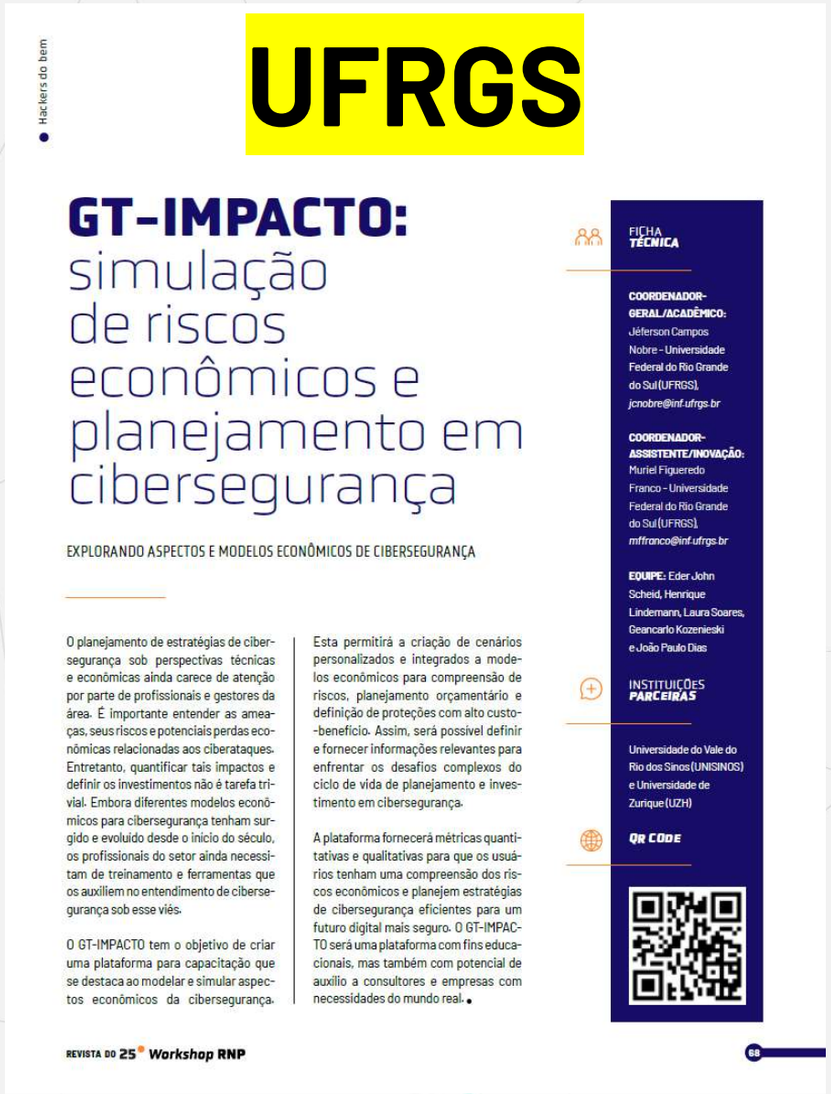
O processo de capacitação em segurança cibernética é bastante desafiador, dados os requisitos de conhecimentos em diferentes subáreas da computação. Por tais motivos, um amplo conjunto de metodologias e estratégias propõe a conciliação entre a teoria e a prática no ensino dos diversos temas existentes, na perspectiva de reduzir a curva de absorção de conceitos técnicos que, muitas vezes, são difíceis de serem materializados.

Nossa proposta tem como objetivo desenvolver a arquitetura HackInSDN, que visa a expandir a capacitação em temas de segurança cibernética em ambientes de testbeds. Trata-se de um pacote de ferramentas que oferecerá um ambiente mais robusto e completo para capacitação em

Revista do WRNP 2024

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

UFRGS



Hackers do bem

GT-IMPACTO: simulação de riscos econômicos e planejamento em cibersegurança

EXPLORANDO ASPECTOS E MODELOS ECONÔMICOS DE CIBERSEGURANÇA

O planejamento de estratégias de cibersegurança sob perspectivas técnicas e econômicas ainda carece de atenção por parte de profissionais e gestores da área. É importante entender as ameaças, seus riscos e potenciais perdas econômicas relacionadas aos ciberataques. Entretanto, quantificar tais impactos e definir os investimentos não é tarefa trivial. Embora diferentes modelos econômicos para cibersegurança tenham surgido e evoluído desde o início do século, os profissionais do setor ainda necessitam de treinamento e ferramentas que os auxiliem no entendimento de cibersegurança sob esse viés.

O GT-IMPACTO tem o objetivo de criar uma plataforma para capacitação que se destaca ao modelar e simular aspectos econômicos da cibersegurança. Esta permitirá a criação de cenários personalizados e integrados a modelos econômicos para compreensão de riscos, planejamento orçamentário e definição de proteções com alto custo-benefício. Assim, será possível definir e fornecer informações relevantes para enfrentar os desafios complexos do ciclo de vida de planejamento e investimento em cibersegurança.

A plataforma fornecerá métricas quantitativas e qualitativas para que os usuários tenham uma compreensão dos riscos econômicos e planejem estratégias de cibersegurança eficientes para um futuro digital mais seguro. O GT-IMPACTO será uma plataforma com fins educacionais, mas também com potencial de auxílio a consultores e empresas com necessidades do mundo real.

FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO: Jéferson Campos Nobre – Universidade Federal do Rio Grande do Sul (UFRGS), *jcnobre@inf.ufrgs.br*

COORDENADOR-ASSISTENTE/INOVAÇÃO: Muriel Figueredo Franco – Universidade Federal do Rio Grande do Sul (UFRGS), *mffranco@inf.ufrgs.br*

EQUIPE: Eder John Scheid, Henrique Lindemann, Laura Soares, Geancarlo Kozenieski e João Paulo Dias

INSTITUIÇÕES PARCEIRAS

Universidade do Vale do Rio dos Sinos (UNISINOS) e Universidade de Zurique (UZH)

QR CODE

REVISTA DO 25º Workshop RNP

68

Revista do WRNP 2024

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

HACKERS DO BEM

Capture the Flag (CTF)

Segunda edição do CTF do Hackers do Bem atrai 281 competidores

Hackatons

2º Hackathon do Hackers do Bem reúne jovens talentos em Natal-RN pa...

Cybergame

Cybergame do Hackers do Bem destaca talentos em cibersegurança no 2...

Outras iniciativas em PESQUISA, DESENVOLVIMENTO & INOVAÇÃO na RNP

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

- COMITÊS TÉCNICOS de Prospecção Tecnológica na RNP

Gestão de Identidade

O Comitê Técnico de Gestão de Identidade (CT-GId) tem por objetivo realizar recomendações técnicas e apresentar uma visão de futuro acerca dos temas relacionados à gestão de identidades, que mais têm merecido a atenção de pesquisadores. Alguns cenários analisados estão em aplicações na área de saúde, federação de nuvens e testbeds, pesquisa em autorização e autenticação, e interoperabilidade de sistemas.

https://www.rnp.br/ct-gid

Ciência de Dados e Inteligencia Artificial

O Comitê Técnico de Ciência de Dados e Inteligência Artificial (CT-CDIA) foi criado pela RNP em 2022 e visa estudar o futuro das aplicações de ciência de dados e I.A., nas mais variadas áreas de pesquisa, mas com ênfase em aplicações de interesse do Sistema RNP, tais como educação, cultura, telemedicina, cibersegurança, redes de computadores e melhorias de processos organizacionais.

Cibersergurança

O Comitê Técnico de Cibersegurança (CT-Cibersegurança), criado em maio de 2024, é um fórum de discussão aberto que visa estruturar uma rede de cooperação envolvendo atores da academia, startups, governo e grupos de trabalho da própria RNP que atuam na área. Busca-se identificar desafios tecnológicos e potenciais projetos de pesquisa e desenvolvimento a serem explorados pelos membros do comitê e pela RNP e propor um documento de visão de futuro para a atuação da RNP em cibersegurança.

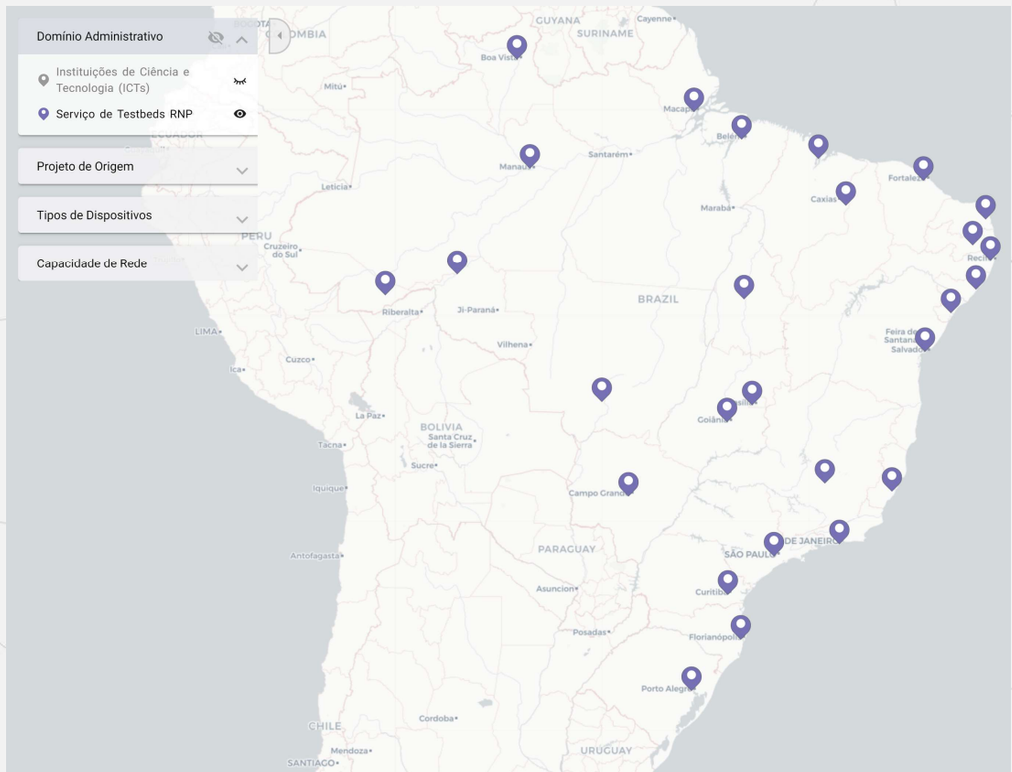
https://www.rnp.br/ct-ciberseguranca

Editais de Financiamento para Projetos de P&D de CURTA DURAÇÃO

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

TESTBEDS

Um GRANDE *"Laboratório Multiusuário"* com infraestrutura computacional distribuída e acessível remotamente para realização de Experimentos, Testes, PoC, Demos em TICs.



Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

*** Minicurso 5 ***
apresentado durante o **42º *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*** (SBRC 2024)

Capítulo

5

Testbeds para Pesquisa Experimental em Cibersegurança: Da Teoria à Prática

Michelle Silva Wangham*‡, Bruno H. Meyer†, Davi D. Gemmer*, Khalil G. Q. de Santana‡, Lucas Rodrigues Frank§, Luiz Eduardo Folly de Campos*, Emerson Ribeiro de Mello¶ e Marcos Felipe Schwarz*

Abstract

The current scenario for experimental research in cybersecurity is promising and broad, encompassing various infrastructures and application domains. However, conducting experiments faces significant challenges, such as high costs, operational risks, resource and network management, heterogeneity, capacity and quantity of devices, flexible experiment orchestration, and a large volume of generated experimental data. This chapter aims to present specialized testbeds for conducting cybersecurity experiments, focusing on the MENTORED Testbed, particularly emphasizing the analysis of vulnerabilities, attacks, and defense strategies associated with Internet of Things devices. This testbed is a controlled environment for experimentation and is used as a case study for hands-on demonstrations of theoretical concepts. This chapter describes two DDoS attack experiments, and their results are presented and analyzed.

Resumo

O cenário atual para pesquisa experimental em cibersegurança é promissor e abrangente, englobando diversas infraestrutura e domínios de aplicação. Porém, a condução de experimentos enfrenta uma série de desafios significativos, tais como altos custos, riscos operacionais, gerenciamento de recursos e de redes, heterogeneidade, capacidade

*Rede Nacional de Ensino e Pesquisa. Email: michelle.wangham@rnp.br, davi.gemmer@rnp.br, luiz.campos@rnp.br, marcos.schwarz@rnp.br
†Universidade Federal do Paraná. Email: bruno.meyer@ufpr.br
‡Universidade do Vale do Itajaí. Email: wangham@univali.br, khalil.santana@edu.univali.br
§Universidade Federal de Juiz de Fora. Email: lucasrodrigues@ice.ufjf.br
¶Instituto Federal de Santa Catarina. Email: mello@ifsc.edu.br

Powered by

TESTBEDS

https://www.rnp.br/servicos/testbeds

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

- **RNP em parceria com o CPqD e a Softex**

P&D em **Aplicações** de Blockchain em áreas estratégicas

P&D em tecnologia e aplicações de **Identidade Digital Descentralizada**

Rede(s) Blockchain para Experimentação e Testes de aplicações + Criação de **TESTBED MULTIPLATAFORMA**

P&D para o **avanço do estado da arte das tecnologias** de Blockchain

Observatório Nacional de Blockchain
+ Capacitações

https://linktr.ee/iliada.blockchain

Iniciativas em Pesquisa, Desenvolvimento & Inovação na RNP

Grupos de trabalho (GTs)

Desde 2002, a RNP lança editais para fomentar Grupos de Trabalho (GTs), a fim de **desenvolver projetos colaborativos com a comunidade acadêmica.**

Boas ideias...

Algumas dessas boas ideias se transformam em serviços consolidados que passam a fazer parte do nosso Catálogo de Serviços e são disponibilizados como produtos para instituições que fazem parte do Sistema RNP!

#ALERTA de #Oportunidade!!

https://www.rnp.br/inovacao/editais

MUITO OBRIGADO(A)

GUSTAVO Neves DIAS
https://www.linkedin.com/in/gndias/
gustavo.dias@rnp.br

RNP
MINISTÉRIO DA CULTURA
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO