Title: Tools for Training White Hat Hackers

Authors: Michelle Wangham (RNP), Rômulo Pinheiro (RNP), Lisandro Granville (RNP) and Iara Machado (RNP)

Cybersecurity demands professionals who constantly learn, adapt to new technologies, solve evolving problems, and anticipate risks. Despite this, there must be more demand for cybersecurity experts and qualified training. In Brazil alone, ISC² reports over 300,000 unfilled cybersecurity positions.

In this context, the White Hat Hackers program (Hackers do Bem in Portuguese) emerged to revolutionize the security landscape in Brazil. The program operates on multiple fronts, nurturing the ecosystem with innovative solutions and bridging cybersecurity professionals to diverse market opportunities. Implemented under Softex's National Priority Innovation Program, the initiative is executed by the National Education and Research Network (RNP) and Senai São Paulo, supported by resources from the ICT Law.

This program is outstanding cybersecurity and privacy skilled human resource development through (i) training actions for the development of skills using intensive experimentation environments, cybersecurity simulators, and technological residencies, (ii) research, development, and innovation (RD&I) actions and (iii) implementation of a national cybersecurity hub. The "Hackers do Bem" virtual learning environment has registered 130 thousand students.

The program has two strategies to foster the cybersecurity innovation ecosystem: coordinate and execute RD&I projects and organize and conduct events (CTFs, hackathons, and workshops on cybersecurity education) to strengthen connections between stakeholders in the cybersecurity ecosystem. The RD&I program aims to bridge critical cybersecurity education gaps, aligning with RNP's dedication to cultivating future professionals and fostering the creation of innovative educational tools to equip professionals for evolving digital security challenges.

In the first open call for the program, we received 40 projects, and after a careful selection phase, we selected seven RD&I projects. Since January, the projects have been under development. Consequently, seven technological artifacts are being developed to promote cybersecurity teaching, accompanied by researchers through Working Groups (WG) that focus on developing open-source solutions, such as simulators, emulating attack, and defense environments, and generating datasets, among others, on advancing the state-of-the-art. These solutions will address challenges in the field of information security, aimed at strengthening advanced training of cybersecurity professionals.

This presentation aims to showcase the outcomes of our program, highlighting RD&I projects and events we have organized, including three Capture the Flag (CTF) competitions, one cybergame, two hackathons, and two workshops. Below is a brief description of the tools being developed in the projects (WGs):

- WG-HIKARI is developing an integrated platform for online defense competitions and threat hunting, providing a practical and interactive environment for cybersecurity training.
- WG-EXSS introduces an educational emulator focused on Cross-Site Scripting (XSS) attacks, enabling practical learning about detecting and mitigating these vulnerabilities.
- WG-ETSC offers a flexible and dynamic emulator for cybersecurity training, enhancing users' practical skills in a secure environment.
- WG-Malware DataLab applies generative artificial intelligence techniques to detect malware, contributing to more robust defenses against advanced cyber threats. Students will be able to experiment, understand and validate different configurations of generative AI models in generating synthetic data.
- WG-HackInSDN adds a cybersecurity training service to the RNP testbeds, using a programmable infrastructure for teaching networks and security.
- WG-IMPACTO explores the economic aspects of cybersecurity, simulating risks and developing strategies to strengthen organizations' security postures.
- WG-CRIVO focuses on the continuous prioritization of vulnerabilities within each organization's context, maximizing the impact of security teams through strategic risk management. These initiatives represent a multidisciplinary effort to address cybersecurity challenges, providing innovative solutions that meet the needs of both the academic and business sectors.

We envision that our presentation will attract the interest of audience members seeking to see how we coordinate RD&I security projects at RNP and know the resulting tools for training white hat hackers. Therefore, we hope that our presentation will motivate other NRENs to promote cybersecurity events to enhance the training of professionals.