**Proposta de TCC**

**MAC0499 - Trabalho de Formatura Supervisionado**

**Responsável: Profa. Nina S. T. Hirata**

**Orientador: Prof. João Eduardo Ferreira**

Daniel de Sousa Martinez – NUSP 10297709

# Introdução

O projeto *Hackers do Bem* consiste em um grupo de alunos do Bacharelado em Ciência da Computação do IME-USP (composto atualmente por Daniel de Sousa Martinez, Cainã Setti Galante, Victor Seiji Hariki e Victor Aristóteles Rocha Campos), responsáveis por avaliar e testar a segurança da infraestrutura de TI da Universidade de São Paulo. Fazendo uso de ferramentas existentes para bug bounties e desenvolvendo nossas próprias, procuramos por bugs conhecidos em aplicações web e escaneamos por vulnerabilidades em servidores da Universidade.

Existem inúmeros tipos de problemas de segurança que um sistema conectado à internet pode apresentar, e por consequência existe uma grande quantidade de ferramentas para encontrá-los, ou até mesmo explorá-los. No entanto, a grande maioria delas ou está restrita a um tipo específico de vulnerabilidade ou não é fácil de ser automatizada para busca em uma grande quantidade de *hosts.*

Portanto, na tentativa de automatizar o trabalho que tem sido feito por nós manualmente, iniciamos o desenvolvimento do VuMoS (USP's Vulnerability Monitoring System), que não somente visa buscar vulnerabilidades de diversos tipos nos mais diversos sistemas da USP, como também monitorar as possíveis correções futuras, além de buscar novas brechas em novos sistemas.

# Objetivo

O objetivo desse trabalho consiste em desenvolver essa ferramenta em conjunto com o *Hackers do Bem*, implementando nele a descoberta de novos *hosts* através de enumeração de *IPs, DNS* e *web crawling*, integração com ferramentas de busca de vulnerabilidades existentes, assim como alertas de novas vulnerabilidades.

# Metodologia

O projeto será desenvolvido utilizando uma arquitetura modular de microsserviços, para que a implementação de novos módulos, tanto de descoberta quanto de análise, seja fácil e independente, podendo ser feitos até mesmo em linguagens diferentes. Cada um desses microsserviços será composto por um *docker container,* orquestrados pelo *docker-compose* para facilitar seu desenvolvimento.

Os dados gerados pelo sistema serão armazenados em um banco de dados relacional (*PostgreSQL*) central, enquanto a comunicação entre os módulos ocorrerá através de um sistema de mensageiria (*NATS*).

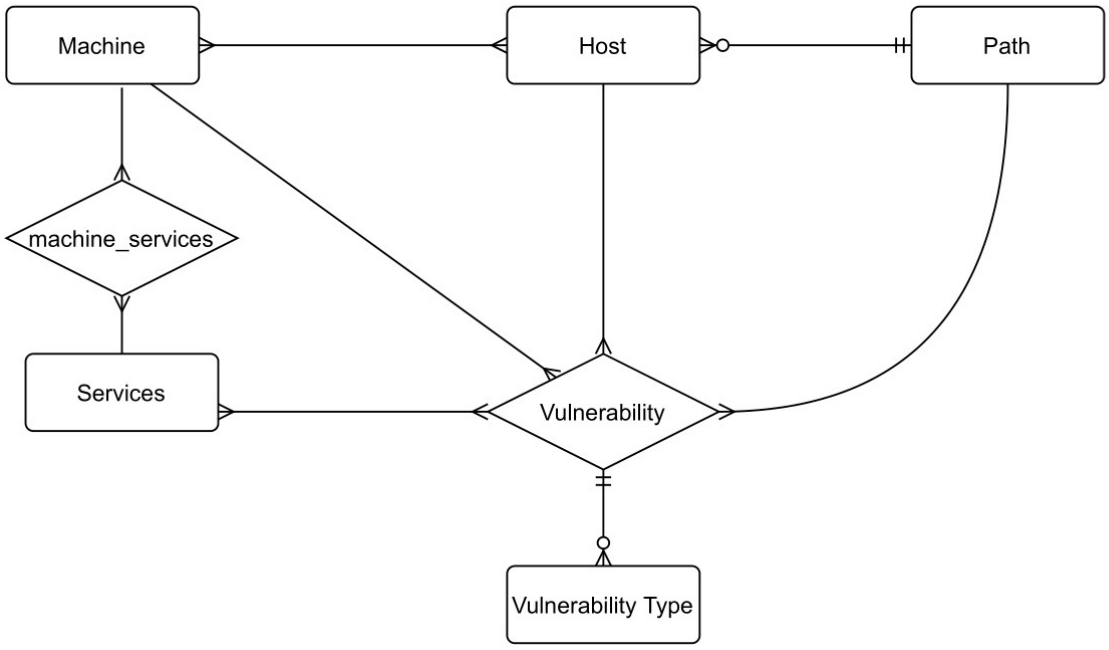


Figura 1: Modelo do banco de dados

Um desses módulos será uma interface *web* que, através do envio e recebimento de mensagens, controlará os outros módulos e exibirá seus respectivos progressos e resultados.

Alguns módulos iniciais a serem implementados serão:

- Amass – Módulo de descoberta, que utiliza a ferramenta *Amass* para enumeração de DNS para encontrar subdomínios.
- Crawler – Módulo de descoberta, que procura novas páginas dinâmicas para cada página/subdomínio encontrados anteriormente.
- Nmap – Módulo de descoberta e análise, que utiliza a ferramenta *Nmap* para encontrar serviços e alguns tipos de vulnerabilidades.
- SQLMap – Módulo de análise, que utiliza a ferramenta *SQLMap* para procurar vulnerabilidades de SQL Injection nos *hosts* e subdomínios encontrados.
- Controle – Módulo que mostra o status e controla as configuração dos outros módulos.
- Metasploit – Módulo que utiliza algumas ferramentas do *Metasploit Framework* para encontrar e explorar vulnerabilidades.

# Cronograma

| Atividades | Abr | Mai | Jun | Jul | Ago | Set | Out | Nov | Dez |
|---|---|---|---|---|---|---|---|---|---|
| Idealização e definição da arquitetura do projeto | x | | | | | | | | |
| Implementação de uma prova de conceito monolítica com os módulos *amass, nmap, sqlmap, crawler* | | x | | | | | | | |
| Refatoração dos módulos para a arquitetura de microsserviços | | x | x | | | | | | |
| Implementação do módulo de controle e configuração | | | x | x | x | | | | |
| Refinamento da aquisição de dados do *Crawler* | | | | | x | | | | |
| Implementação do módulo *Metasploit* | | | | | | x | x | | |
| Estudo e refinamento da efetividade do sistema | | | | | | | x | | |
| Desenvolvimento da monografia | | | | | | | x | x | x |
| Finalização do projeto | | | | | | | | x | x |
| Preparação da apresentação | | | | | | | | | x |