CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA
CELSO SUCKOW DA FONSECA - CEFET/RJ *CAMPUS*
PETRÓPOLIS
CURSO DO BACHARELADO EM ENGENHARIA DE
COMPUTAÇÃO

PROPOSTA DO TRABALHO DE CONCLUSÃO DE CURSO

Pedro Carneiro Pizzi

26 de janeiro de 2025

1 Disposições Gerais

As disposições gerais do Trabalho de Conclusão de Curso (TCC), a ser completado na disciplina TCC II, correspondem a:

- Título: Detecção de ataques *DoS* utilizando IA Generativa;
- Modalidade: Acadêmico;
- Orientador: Dalbert Marcharenhas;

2 Tema

O trabalho propõe uma análise da detecção de ataques do tipo *DoS* (*Denial of Service*) utilizando Inteligência Artificial Generativa. A abordagem emprega o modelo *Llama*, com foco na identificação de padrões em capturas de pacotes realizadas em simulações de ataques. O objetivo principal é avaliar a eficácia do modelo antes e após a realização de um *fine-tuning*, visando aprimorar a precisão na detecção. Além disso, busca-se comparar os resultados obtidos com soluções comerciais amplamente utilizadas, explorando o potencial da IA generativa no contexto da segurança de sistemas.

3 DELIMITAÇÃO

O objeto de estudo deste trabalho são os pacotes de rede capturados em simulações de ataques DDoS (*Distributed Denial of Service*). As simulações serão realizadas em um ambiente controlado, utilizando duas máquinas virtuais e um computador real, configurados para reproduzir cenários reais de ataque. O objetivo é detectar, em tempo real, se está ocorrendo um ataque DDoS, utilizando o modelo *Llama* para identificar padrões de tráfego malicioso.

A arquitetura proposta processará os dados de tráfego capturados durante as simulações nas máquinas virtuais. O foco será na detecção de ataques DDoS específicos, simulados de forma a representar situações relevantes no contexto de segurança de redes.

Para aprimorar a eficácia do sistema, será realizada uma análise do desempenho do modelo *Llama* na detecção de possiveis ataques, antes e após o *fine-tuning*, buscando otimizar a performance em tarefas de detecção e classificação [3]. Além disso, os resultados obtidos serão comparados com soluções comerciais disponíveis no mercado, destacando as vantagens e limitações do uso de IA Generativa no contexto da segurança de sistemas.

4 JUSTIFICATIVA

Com o avanço da Internet, a crescente complexidade das redes de computadores e a ascensão da inteligência artificial generativa, a segurança de redes tornou-se ainda mais crucial. A IA generativa, com seu vasto potencial, pode ser empregada tanto para fortalecer sistemas de segurança quanto para criar ameaças mais sofisticadas. Assim, a implementação de soluções de segurança robustas e inteligentes em qualquer arquitetura é indispensável para proteger computadores e dispositivos contra uma ampla variedade de ataques e vulnerabilidades, muitas vezes impulsionados por avanços tecnológicos. Ligado a isso, ataques de negação de serviço representam não apenas uma ameaça técnica, mas também econômica, impactando severamente empresas e serviços críticos [1].

Nessa linha, no cenário atual de cibersegurança, onde ataques são projetados para explorar as menores brechas, o uso de modelos preditivos robustos torna-se essencial para prevenir danos em larga escala. Com a evolução contínua das técnicas empregadas por cibercriminosos, é fundamental contar com soluções de segurança avançadas, como o uso de inteligência artificial, para detectar e mitigar essas ameaças de maneira eficaz e proativa [2].

Diante dos fatos apresentados, este trabalho tem como objetivo analisar o tráfego de rede de um servidor em tempo real, com o intuito de detectar possíveis ataques de negação de serviço (DoS) com base no fluxo de pacotes observados. A proposta inclui a implementação de medidas defensivas, bloqueando a comunicação de usuários suspeitos e protegendo o sistema. Para isso, será utilizado o modelo LLaMA, ajustado por meio de fine-tuning, permitindo maior precisão na detecção. Os resultados obtidos serão comparados com ferramentas de mercado, buscando avaliar o desempenho e a eficácia da abordagem proposta. Nesse contexto, a comparação de soluções baseadas em inteligência artificial com sistemas comerciais permite identificar lacunas e oportunidades de melhoria, promovendo inovações na área de cibersegurança [4].

5 Objetivo

O objetivo principal deste trabalho é criar uma ferramenta de Prevenção de Intrusões (IPS) que seja moderna, intuitiva e fácil de usar. A proposta inclui o uso de Inteligência Artificial Generativa para otimizar o processo de detecção e resposta a ameaças, eliminando a complexidade associada à instalação e configuração de sistemas IPS tradicionais, tornando a solução mais acessível e eficiente para diversos usuários.

Para avaliar o desempenho da ferramenta, o objetivo é compará-la com soluções disponíveis no mercado, além de analisar sua eficiência por meio da detecção de ataques simulados.

6 Metodologia

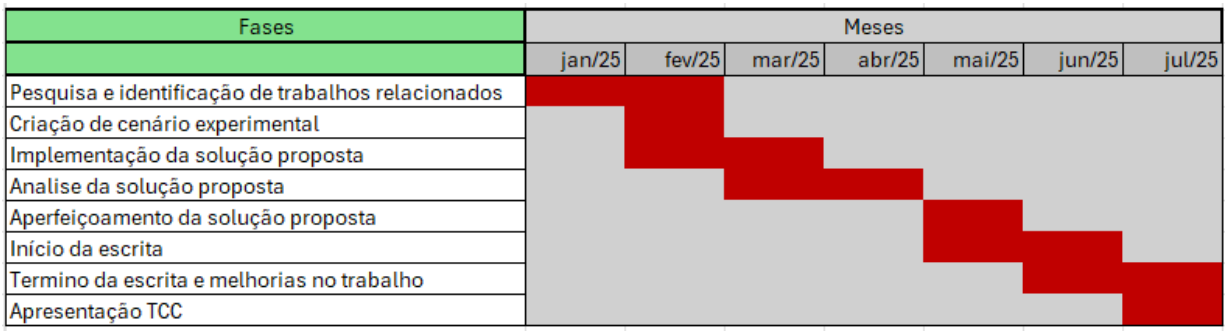
Diferentes cenários de simulação de ataques e de navegação normal foram testados para avaliar a eficiência na detecção de possíveis ataques DoS, mesmo sem realizar o fine-tuning no modelo. Após medir a eficiência inicial, o fine-tuning será realizado para aprimorar a detecção e avaliar seu desempenho. Além disso, será configurado o bloqueio automatico dos indivíduos suspeitos quando ataques forem detectados. Por fim, será realizada uma comparação com softwares de mercado, com o objetivo de medir a eficiência da solução proposta.

7 Materiais

Para desenvolver a ferramenta proposta, foi criado um ambiente de simulação de ataques utilizando duas máquinas virtuais com sistema operacional Lubuntu: uma com um servidor Apache configurado como alvo e outra simulando um atacante utilizando softwares para geração de ataques DoS. Além disso, um computador físico com sistema operacional Windows foi utilizado como servidor, sendo responsável por receber, processar e responder aos pacotes, realizar análises e responder às requisições por meio do modelo Llama.

8 Cronograma

Figura 8.1: Cronograma TCC



- Fase 1 : Pesquisa e identificação de trabalhos relacionados - Jan/2025 até Fev/2025
- Fase 2 : Criação de cenário experimental - Fevereiro/2025
- Fase 3 : Implementação da solução proposta - Fevereiro/2025 até Março/2025
- Fase 4 : Analise da solução proposta - Março/2025 até Abril/2025
- Fase 5 : Aperfeiçoamento da solução proposta - Maio/2025
- Fase 6 : Início da escrita - Maio/2025 até Junho/2025
- Fase 7 : Termino da escrita, Melhorias no trabalho - Junho/2025 - Julho/2025
- Fase 8: Apresentação TCC - Julho/2025

REFERÊNCIAS

[1] ANDERSON, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020. "Denial-of-service attacks represent not only a technical threat but also an economic one, severely impacting companies and critical services."

[2] KOLACZYK, Eric D.; CSÁRDI, Gábor. Statistical Analysis of Network Data with R. New York: Springer, 2014. "In the current cybersecurity landscape, where attacks are designed to exploit even the smallest gaps, the use of robust predictive models becomes essential to prevent large-scale damage."

[3] GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. Cambridge: MIT Press, 2016. "The adaptation of pre-existing models through fine-tuning techniques is an effective strategy to address specific problems, optimizing performance in detection and classification tasks."

[4] SZPANKOWSKI, Wojciech. Information Theory and Network Security. Cambridge: Cambridge University Press, 2018. "The comparison of artificial intelligence-based solutions with commercial systems allows for identifying gaps and improvement opportunities, fostering innovation in the field of cybersecurity."