

# **Projeto da disciplina Redes de Computadores**

**Professor: Iguatemi Eduardo da Fonseca**

**Tema: Sistema de Detecção de Intrusão (IDS)**

**Participantes:**

**Thaís Melquíades Macêdo (20190021376);**

**Vinícius Germano de Barros (20220096650)**

O objetivo é desenvolver um sistema capaz de detectar atividades suspeitas na rede, como tentativas de ataques ou acessos não autorizados, analisando o tráfego de pacotes em tempo real utilizando um sniffer capturando esses pacotes de rede. Podemos identificar padrões suspeitos, como múltiplas tentativas de conexão (ataque de força bruta), padrões de tráfego incomuns (indicando possível ataque DDoS), pacotes malformados ou com assinaturas conhecidas de ataques. O intuito é também enviar notificações ao detectar um comportamento suspeito, criando um painel simples para visualizar estatísticas e alertas em tempo real.

Por esse projeto podemos demonstrar a aplicação prática de segurança em redes explorando conceitos de detecção de ameaças e análise de tráfego, definindo padrões de ataques, analisando pacotes em tempo real e criando alertas. Por exemplo: O IDS escuta o tráfego da rede e armazena os IPs que enviam pacotes. A cada 10 segundos, ele verifica quantos pacotes cada IP enviou, se um IP ultrapassar um limite (ex: 100 pacotes em 10s), ele será marcado como suspeito e um alerta será gerado.