ĐẠI HỌC BÁCH KHOA HÀ NỘI

TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

———————— * ————————

ĐỀ XUẤT ĐỒ ÁN

Môn học: Project II (IT - 3931)

Đề tài: Network Security with IDS/IPS: Detection and Prevention of Network Attacks in a Virtualized Environment

Sinh viên thực hiện: **Ngô Trung Hiếu - 20225316**

Kỹ thuật máy tính 04 – K67

Giảng viên hướng dẫn: **Nguyễn Quốc Khánh**

Hà Nội – 2025

Mục lục

I. Tên đề tài

Network Security with IDS/IPS: Detection and Prevention of Network Attacks in a Virtualized Environment

II. Mục tiêu

1. Xây dựng một môi trường mạng ảo mô phỏng tấn công và phòng thủ.
2. Cài đặt và cấu hình **IDS/IPS (Snort hoặc Suricata)** để phát hiện các mối đe dọa mạng phổ biến.
3. Phát triển một số **rule tùy chỉnh** để nhận diện các loại tấn công như port scanning, brute-force, DoS, SQL injection.
4. Đánh giá hiệu quả của IDS/IPS trong việc phát hiện và chặn tấn công.

III. Phạm vi và giới hạn

1. Phạm vi:
- Mô phỏng trên máy ảo (VirtualBox/VMware).
- Gồm 3–4 node: attacker (Kali Linux), victim (Ubuntu Server), IDS/IPS node.

2. Giới hạn:
- Không triển khai trên hệ thống thực tế.
- Chỉ tập trung vào một số kiểu tấn công phổ biến.
- IDS/IPS dựa trên rule, chưa tích hợp Machine Learning.

IV. Phương pháp thực hiện

1. Tìm hiểu lý thuyết: IDS/IPS, cơ chế rule-based detection, inline vs passive.
2. Triển khai môi trường lab:
- Xây dựng topology mạng ảo.
- Cài đặt IDS/IPS (Snort/Suricata).
3. Thực hiện thí nghiệm:
- Sinh traffic bình thường và traffic tấn công (nmap scan, brute force, DoS, SQLi).
- Thu thập log, alert.

4. Phân tích kết quả:
- Đánh giá khả năng phát hiện.
- Nhận xét false positive/false negative.

V. Kết quả dự kiến

- Báo cáo: Tổng hợp lý thuyết, triển khai, thử nghiệm, kết quả.
- Topology mạng ảo: Sơ đồ và file cấu hình lab.
- Bộ rule IDS/IPS: Rule viết tay + rule mặc định.
- Kết quả log/alert: Minh chứng IDS/IPS phát hiện/chặn tấn công.
- Slide thuyết trình + Demo: Trình bày cho giảng viên.

VI. Project repository và thông tin liên lạc

- **Github:** https://github.com/ngo-hieu-7733/Project-IT3931-Network-Security-with-IDS-IPS
- **MS Teams:** hieu.nt225316@sis.hust.edu.vn