

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP. HCM**  
**KHOA CÔNG NGHỆ THÔNG TIN**

-----🙞🙜🕮🙞🙜-----

**ĐỒ ÁN 1**

**XÂY DỰNG HỆ THỐNG IPS**

**DÙNG HIDS-OSSEC**



GVHD: Nguyễn Hoà

Sinh viên thực hiện:  
1. Phạm Văn Duẩn (13037321)

2. Võ Thành Luân()

3. Mai Quốc Quy ()

4. …Vinh ()

*TP. Hồ Chí Minh, tháng 5 năm 201**6*

1. **Đặt vấn đề**
   1. **Tầm quan trọng của IDS**
   2. **Vai trò của HIDS**
   3. **Bài toán đặt ra của đề tài**
2. **Mô hình hệ thống và phương pháp thực hiện**
   1. **Mô hình hệ thống**
   2. **Công nghệ thực hiện**
   3. **Phương pháp thực hiện**
3. **Các module phân tích và xử lý log của đề tài**
   1. **Nhận dạng log**
   2. **Lấy log từ workstation**
   3. **Decode log**
   4. **Rule**
   5. **Alert và Active Reponse**
4. **Kết quả thực hiện**
   1. **Kết quả đạt được**
   2. **Hạn chế**
5. **Hướng phát triển**