TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG
THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

DANH SÁCH ĐỀ TÀI ĐỒ ÁN CHUYÊN NGÀNH NGÀNH ATTT HỌC KỲ I NĂM HỌC 2025-2026

STT ĐỀ TÀI	TÊN ĐỀ TÀI	NỘI DUNG YÊU CẦU	GIÁO VIÊN HƯỚNG DẪN	EMAIL	BỘ MÔN	GHI CHÚ
1	Thiết kế và cài đặt hệ thống mạng cho doanh nghiệp có 3 chi nhánh trên nền tảng Windows Server 2025	- Thiết kế và cài đặt hệ thống mạng cho doanh nghiệp có 3 chi nhánh với các yêu cầu sau: Thiết kế + Phân hoạch IP + Thiết kế mô hình IP + Thiết kế mô hình logic + Thiết kế OU và GPO + Thiết kế DNS, Active Directory, DHCP + Thiết kế File Services. + Sites & Replication: định nghĩa Subnet/Site Link, lịch replication. + Bảo mật: phân quyền quản trị theo chi nhánh, cấu hình GPO, bật Audit & Logging. Cài đặt và cấu hình + Cài đặt Windows Server 2025, cấu hình IP tĩnh, DNS, NTP. + Promote Domain Controller cho domain cha và các domain con. + Cấu hình Sites/Subnets trong AD Sites and Services. + Cấu hình DNS, DHCP, DFS, VPN. + Tạo OU, User, Group, GPO để kiểm soát chính sách. + Thử nghiệm join máy trạm từ 3 chi nhánh vào domain. Kiểm tra + Kiểm tra đăng nhập từng chi nhánh. + Kiểm tra DNS resolution, DHCP cấp phát IP, replication giữa các DC. + Kiểm tra failover DHCP, restore System State DC. + Đo hiệu suất: thời gian đăng nhập, tốc độ replication, tính ổn định VPN. + Đánh giá mức độ bảo mật, quản lý tập trung, khả năng mở rộng. Kết quả đạt được + Xây dựng thành công mô hình mạng doanh nghiệp đa chi nhánh trên Windows Server 2025.	Ngô Quốc Huy	huynq@huit.edu.vn	MMT&ATTT	
2	Xây dựng mô hình phát hiện xâm nhập bằng thuật toán hồi quy logistic trong học máy	- Thu thập và chuẩn bị dữ liệu - Tiền xử lý dữ liệu: Làm sạch và chuyển đổi dữ liệu để mô hình hiểu được. - Phân chia dữ liệu: Chia dữ liệu thành bộ dữ liệu huấn luyện và kiểm thử. - Huấn luyện mô hình: Huấn luyện mô hình Hồi quy Logistic trên bộ dữ liệu huấn luyện. - Đánh giá Mô hình: Kiểm tra mô hình hoạt động tốt trên tập dữ liệu mới.	Ngô Quốc Huy	huynq@huit.edu.vn	MMT&ATTT	

STT ĐỀ TÀI	TÊN ĐỀ TÀI	NỘI DUNG YÊU CẦU	GIÁO VIÊN HƯỚNG DẪN	EMAIL	BỘ MÔN	GHI CHÚ
3	Xây dựng môi trường Honeypot mô phỏng hệ thống IoT/Smart Home để thu thập và phân tích các mối đe dọa an ninh mạng	- Tìm hiểu các lỗ hổng bảo mật phổ biến trên thiết bị IoT : mật khẩu mặc định, dịch vụ không an toàn như Telnet, lỗ hổng firmware,... và các kỹ thuật tấn công đặc thù. - Thiết kế kiến trúc Honeypot, lựa chọn và triển khai các công cụ giả lập dịch vụ IoT: Cowrie, Dionaea ,.... - Sử dụng máy ảo hoặc container (Docker) để tạo một môi trường cô lập, an toàn. - Triển khai Honeypot lên môi trường mạng (Internet) để bắt đầu thu hút và ghi lại các hoạt động tấn công: địa chỉ IP nguồn, các lệnh được thử, các tệp tin/mã độc được tải lên. - Phân tích log, các mẫu mã độc thu thập được để xác định xu hướng tấn công : các quốc gia tấn công nhiều nhất, mật khẩu phổ biến được sử dụng,.... - Xây dựng một dashboard (bảng điều khiển) để trực quan hóa dữ liệu tấn công theo thời gian thực.	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT	
4	Threat Hunting trên framework MITRE ATT&CK: Phân tích Log để phát hiện dấu vết của Tấn công có chủ đích trong môi trường giả lập.	-Tìm hiểu sâu về framework MITRE ATT&CK cùng các kỹ thuật, chiến thuật và quy trình của hacker. Tìm hiểu cách hacker xâm nhập, duy trì quyền truy cập, leo thang đặc quyền. - Triển khai một hệ thống quản lý và phân tích log (SIEM). Lựa chọn ELK Stack (Elasticsearch, Logstash, Kibana) hoặc Splunk Free. Đây là các công cụ mà doanh nghiệp thực tế đang sử dụng. - Tìm và tải về một bộ dữ liệu có sẵn được thiết kế cho việc thực hành Threat Hunting, gợi ý dùng Mordor cung cấp log Windows Event Logs từ một môi trường đã bị tấn công giả lập. Đưa bộ dữ liệu này vào hệ thống SIEM để phân tích - Dựa trên kiến thức về MITRE ATT&CK tạo ra các giả thuyết về các chiến thuật, kịch bản hacker đã tấn công, và tiến hành viết các truy vấn trên Kibana, Splunk để tìm log chứng minh giả thuyết đã đưa ra. - Sau khi có bằng chứng cụ thể, trình bày viết báo cáo điều tra theo mẫu tiêu chuẩn (Phân tích SOC level 1, 2) sinh viên tìm hiểu được gồm: mô tả từng bước của cuộc tấn công, cung cấp minh chứng cụ thể (logs) cho từng phát hiện, ánh xác các hành vi với các kỹ thuật trong MITRE ATT&CK. - Đưa ra các qui tắc pphát hiện mới để SIEM có thể tự cảnh báo hành vi tương tự và thực hiện kiểm thử sau khi đưa các dectection rules này vào SIEM.	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT	
5	Ứng dụng Machine Learning để nâng cao độ chính xác định vị trong nhà dựa trên dữ liệu WiFi RSSI	**Nội dung thực hiện:** 1. Tổng quan về các phương pháp học máy cho hệ thống định vị trong nhà dựa trên kỹ thuật WiFi Fingerprinting. 2. Thu thập dữ liệu RSSI từ các Access Point tại phòng Lab (https://github.com/luongnt1983/IPS) 3. Xử lý và chuẩn hóa dữ liệu (lọc nhiễu, trích chọn đặc trưng). 4. Huấn luyện mô hình AI (thuật toán KNN, Random Forest). 5. So sánh kết quả định vị với phương pháp truyền thống. 6. Đánh giá sai số định vị và đề xuất cải thiện. 7. Kết luận.	TS. Dương Bảo Ninh	ninhdb@huit.edu.vn	MTT&ATTT	

STT ĐỀ TÀI	TÊN ĐỀ TÀI	NỘI DUNG YÊU CẦU	GIÁO VIÊN HƯỚNG DẪN	EMAIL	BỘ MÔN	GHI CHÚ
6	Nghiên cứu sử dụng Deep Learning để định vị trong nhà dựa trên dấu vân tay WiFi	**Nội dung thực hiện:** 1. Tổng quan về các phương pháp học sâu cho hệ thống định vị trong nhà dựa trên kỹ thuật WiFi Fingerprinting. 2. Xây dựng Dataset Fingerprinting WiFi (https://github.com/luongnt1983/IPS). 3. Áp dụng CNN hoặc LSTM để dự đoán vị trí định vị. 4. So sánh kết quả định vị với KNN truyền thống. 5. Đánh giá độ chính xác và thời gian tính toán. 6. Kết luận.	TS. Dương Bảo Ninh	ninhdb@huit.edu.vn	MTT&ATTT	

Người lập

Lương Thị Quỳnh Mai

Trưởng khoa

Nguyễn Hồng Vũ