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 (1TC) HỌC KỲ II NĂM HỌC 2025-2026

STT ĐỀ TÀI	TÊN ĐỀ TÀI	NỘI DUNG YÊU CẦU	GIÁO VIÊN HƯỚNG DẪN	EMAIL	BỘ MÔN	Định hướng đề tài (Ứng dụng, Nghiên cứu, Kết hợp,	GHI CHÚ
1	Nghiên cứu và triển khai Pentesting trên Android Applications	- Nghiên cứu các loại lỗ hổng - Nghiên cứu các kỹ thuật pentesting trên Android Applications - Nghiên cứu và triển khai các kỹ thuật: + Kỹ thuật phân tích tĩnh + Kỹ thuật dịch ngược (bên trong APK, Smali, Patchinh ứng dụng Android) + Kỹ thuật phân tích động + Tìm hiểu và triển khai kiểm thử trên bộ công cụ Hooking với Frida	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT	Ứng dụng	
2	Tìm hiểu kỹ thuật khai thác lỗ hổng bảo mật bằng công cụ Metasploit	-Tìm hiểu các phương pháp khai thác lỗ hổng bảo mật trong hệ thống mạng như dịch vụ web, dns... - Tìm hiểu chức năng, đặc điểm của công cụ Metasploit - Tìm hiểu, triển khai các tính năng khai thác lỗ hổng, thu thập thông tin, Duy trì trạng thái truy cập, Kiểm thử tự động v.v.. - Phân tích và triển khai vào ứng dụng thực tế với yêu cầu xây dựng trên nền tảng mạng quy mô vừa - So sánh với các công cụ khác như: Nmap, Burp Suite, Nessus ... - Kết hợp công cụ phân tích gói tin Wireshark để đánh giá kết quả triển khai	Phạm Nguyễn Huy Phương	phuongpnh@huit.edu.vn	MMT&ATTT	Ứng dụng	
3	Nghiên cứu và triển khai thực nghiệm hệ thống mạng SDN	- Nghiên cứu tổng quan về mạng SDN, kiến trúc và nguyên lý hoạt động. - Phân tích sự khác biệt giữa mạng truyền thống và mạng SDN. - Nghiên cứu giao thức OpenFlow và vai trò của SDN Controller. - Thiết kế mô hình mạng SDN phục vụ triển khai thực nghiệm. - Lựa chọn công cụ triển khai như Mininet và Open vSwitch. - Cài đặt và cấu hình SDN Controller phù hợp. - Triển khai mô hình mạng SDN theo thiết kế đề xuất. - Xây dựng và tích hợp chức năng bảo mật cơ bản trên SDN. - Thực nghiệm, đánh giá hiệu năng và mức độ an toàn của hệ thống. - Phân tích kết quả và đề xuất hướng phát triển, mở rộng hệ thống SDN bảo mật.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT	Ứng dụng	

4	Nghiên cứu và triển khai thuật toán AES-GCM trong bảo mật lưu trữ dữ liệu cục bộ	– Tìm hiểu sâu về thuật toán AES và các chế độ hoạt động (Block Cipher Modes), tập trung phân tích ưu điểm của GCM so với các chế độ truyền thống như CBC hay CTR (về hiệu năng song song hóa và tính năng xác thực). – Nghiên cứu và cài đặt các chuẩn sinh khóa an toàn từ mật khẩu (Key Derivation Function - như PBKDF2 hoặc Argon2) để bảo vệ khóa mã hóa chính. – Xây dựng cấu trúc file lưu trữ bao gồm: Header (Salt, Nonce/IV), Payload (Ciphertext) và Authentication Tag. – Xây dựng phần mềm (trên PC hoặc Mobile) cho phép người dùng chọn file/thư mục để mã hóa và giải mã an toàn sử dụng AES-GCM. – Demo kịch bản tấn công sửa đổi dữ liệu (Bit-flipping attack) trên file đã mã hóa và chứng minh hệ thống phát hiện được sự thay đổi (xác thực thất bại). – Đo lường tốc độ mã hóa/giải mã (Throughput), mức tiêu thụ CPU/RAM khi xử lý các file kích thước lớn (Big Data). So sánh hiệu năng với AES-CBC và HMAC.	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT&ATTT	Ứng dụng	
5	Nghiên cứu kỹ thuật thủy vân số và xây dựng ứng dụng bảo vệ bản quyền ảnh số	-Tìm hiểu về các kỹ thuật che giấu tập tin : + Tìm hiểu phương pháp và mô hình thủy vân số + Tìm hiểu về các thuật toán thủy vân theo miền không gian ảnh (SW; WU-LEE; LBS; PCT) +Tìm hiểu về các thuật toán thủy vân theo mền tần số (DCT; DWT) - Xây dựng chương trình được dùng để nhúng ảnh vào một ảnh gốc nhằm bảo vệ bản quyền số của tác giả bao gồm các chức năng: + Nhận ảnh gốc + Nhận ảnh cần thủy vân + Nhúng thủy vân + Trích xuất thủy vân + Tấn công nhiễu + Thủy vân bằng Phương pháp LSB + Thủy vân bằng Phương pháp DWT + Thủy vân bằng Phương pháp DCT - So sánh tính bền vững của dấu thủy vân giữa 3 phương pháp LSB, DCT và DWT bằng việc thêm tấn công nhiễu với ảnh đã được nhúng thủy vân	Phạm Văn Phùng, Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT	Ứng dụng	
6	Xây dựng module lưu trữ mật khẩu an toàn sử dụng giải thuật Argon2 và cơ chế chống tấn công vét cạn	- Nghiên cứu lý thuyết về hàm băm một chiều, Salt, Pepper và các điểm yếu của các thuật toán cũ (MD5, SHA-1). - Phân tích cấu trúc của Argon2i, Argon2d và Argon2id để lựa chọn biến thể phù hợp cho mục đích lưu trữ. - Thiết kế thuật toán giới hạn tốc độ đăng nhập (Rate Limiting) và cơ chế khóa tài khoản tạm thời (Account Lockout) hoặc CAPTCHA khi phát hiện dấu hiệu vét cạn. - Xây dựng môi trường thử nghiệm để mô phỏng các cuộc tấn công băm mật khẩu bằng GPU/CPU cường độ cao. - Lập trình module bằng ngôn ngữ Python (thư viện argon2-cffi) hoặc Node.js. - Đánh giá hiệu năng và độ an toàn của hệ thống dựa trên thời gian xử lý và khả năng kháng lại các thiết bị phần cứng chuyên dụng (ASIC/FPGA).	Lê Anh Tuấn	tuanla@huit.edu.vn	MMT&ATTT	Nghiên cứu	

NGƯỜI LẬP

Lương Thị Quỳnh Mai

KT. TRƯỞNG KHOA
PHÓ TRƯỞNG KHOA

Nguyễn Thị Bích Ngân