DANH SÁCH KHÓA LUẬN CỬ NHÂN NGÀNH CNTT - HỌC KỲ 1 NĂM HỌC 2025 - 2026

STT	Tên đề tài	Yêu cầu	GVHD	Email	Bộ môn	Định hướng đề tài (Ứng dụng, Nghiên cứu, Kết hợp, MMT)	Ghi chú
1	NGHIÊN CỨU GIẢI PHÁP VELOCIRAPTOR VÀ ỨNG DỤNG TRONG ĐIỀU TRA, ỨNG PHÓ SỰ CỐ AN TOÀN MẠNG	Khảo sát nguyên lý hoạt động, các tính năng của Velociraptor (thu thập dữ liệu điểm cuối, phân tích log, tự động hóa phản ứng). Triển khai môi trường lab để mô phỏng sự cố (truy cập trái phép, đánh cắp dữ liệu) trên máy ảo/container. Đánh giá hiệu quả phát hiện và phản ứng của Velociraptor qua các kịch bản tấn công. Đề xuất cải tiến tích hợp Velociraptor với các công cụ khác. Báo cáo lý thuyết, triển khai, và kết quả kiểm thử,	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
2	NGHIÊN CỨU GIẢI PHÁP AN TOÀN CHO MẠNG KHÔNG DÂY DỰA TRÊN CÔNG CỤ MÃ NGUỒN MỞ NETALERT X	Khảo sát mối đe dọa mạng không dây (rogue AP, unauthorized access). Phân tích tính năng giám sát của NetAlertX (phát hiện thiết bị trái phép, hành vi bất thường). Triển khai NetAlertX trên máy chủ Ubuntu, mô phỏng mạng Wi-Fi bằng OpenWRT và thiết bị giả lập (QEMU). Kiểm thử khả năng phát hiện qua tấn công rogue AP (Aircrack-ng). Đề xuất giải pháp bảo mật (WPA3, network segmentation) và báo cáo kết quả.	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
3	NGHIÊN CỨU VÀ XÂY DỰNG CÁC KỊCH BẢN TẤN CÔNG PHỤC VỤ ĐÀO TẠO AN TOÀN THÔNG TIN TRÊN HỆ THỐNG THAO TRƯỜNG MẠNG CYBER RANGE	Khảo sát các loại tấn công mạng (brute force, privilege escalation, data exfiltration). Thiết kế tối thiểu 3 kịch bản tấn công giáo dục trên Cyber Range (Kali Linux, Metasploitable). Triển khai và kiểm thử kịch bản qua các buổi đào tạo thử nghiệm. Đánh giá hiệu quả nâng cao kỹ năng phát hiện và ứng phó của học viên. Báo cáo lý thuyết, triển khai, kết quả kiểm thử, và đề xuất cải tiến	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
4	NGHIÊN CỨU GIẢI PHÁP ĐIỀU PHỐI ỨNG CỨU TỰ ĐỘNG SỰ CỐ AN TOÀN THÔNG TIN SOAR	Khảo sát tính năng SOAR (TheHive, Shuffle) trong tự động hóa và điều phối ứng cứu sự cố. Triển khai TheHive/Shuffle trên máy ảo/container để mô phỏng sự cố (truy cập trái phép, đánh cắp dữ liệu). Cấu hình workflow tự động (chặn IP, gửi cảnh báo) và kiểm thử hiệu quả. Đề xuất cải tiến tích hợp SOAR với các công cụ khác. Báo cáo lý thuyết, triển khai, kết quả kiểm thử,	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
5	NGHIÊN CỨU TRIỂN KHAI CÔNG CỤ PHÂN TÍCH TẤN CÔNG MẠNG THOR	Khảo sát tính năng của THOR (YARA/Sigma rules, IOCs, anomaly detection). Triển khai THOR trên máy ảo/container để phân tích tấn công (brute force, privilege escalation, data exfiltration). Mô phỏng tấn công bằng Kali Linux và Metasploitable, thu thập và phân tích log. Đánh giá hiệu quả phát hiện và đề xuất cải tiến. Báo cáo lý thuyết, triển khai, kết quả kiểm thử	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
6	NGHIÊN CỨU CÁC KỸ THUẬT VÀ CÔNG CỤ TẤN CÔNG LATERAL MOVEMENT TRONG MÔI TRƯỜNG MẠNG	Nghiên cứu mối đe dọa mạng (C2, data exfiltration). Cấu hình Zeek, Moloch để giám sát lưu lượng mạng. Mô phỏng tấn công Lateral Movement (RDP, PowerShell, credential theft) bằng Metasploit. Phân tích log, đánh giá hiệu quả phát hiện và đề xuất biện pháp ứng phó (network segmentation, MFA). Báo cáo lý thuyết, triển khai, kết quả kiểm thử	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT		
7	An toàn thông tin trên dịch vụ Web, phân tích rủi ro và giải pháp phòng tránh	Tổng quan về kiến trúc Web Application •Tổng quan về Cơ sở dữ liệu •Tổng quan về các lỗ hổng của Web Application •Tổng quan về các rủi ro liên quan đến Web Application •Tổng quan về các kỹ thuật tấn công Web Application và Web server. •Tổng quan về các công cụ khai thác lỗ hổng SQL Injection, XSS, Web phishing; file upload; trên Web Application; * Xây dựng Website thực hiện kịch bản tấn công, phòng thủ.	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT&ATTT		
8	Tìm hiểu về tấn công giả mạo Web Phishing - Xây dựng giải pháp cho các sự cố giả mạo Website	- Tìm hiểu Kỹ thuật tạo web phishing: oTyposquatting oCloning trang hợp pháp oFake HTTPS, chứng chỉ giả •Phân tích cách người dùng bị lừa qua các trang đăng nhập giả •Nhận diện phishing thông qua URL, mã nguồn HTML, favicon, JS obfuscation •Giải pháp bảo vệ: Web filter, DNS filter, phần mềm EDR •Mô phỏng tạo một trang đăng nhập giả (dùng trong môi trường lab). •Dò tìm các dấu hiệu phishing trong trang web. •Triển khai công cụ kiểm tra URL (PhishTank, URLScan.io).	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT&ATTT		

9	Xây dựng cơ chế xác thực 2 nhân tố (2FA) kết hợp OTP cho hệ thống Website	-Tìm hiểu về cơ chế xác thực đăng nhập, - Phân loại và phân tích chi tiết các cơ chế xác thực phổ biến (một yếu tố, hai yếu tố, đa yếu tố). -Tìm hiểu về phương pháp sinh mã (HOTP , TOTP) -Xây dựng hệ thống xác thực 2 lớp (Xây dựng website, ứng dụng đọc mã OTP/ QR, xác thực tin nhắn bằng Email/ Điện thoại di động	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT& ATTT		
10	Ứng dụng trí tuệ nhân tạo trong phát hiện hình thức tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS	- Tìm hiểu về hình thức tấn công từ chối dịch vụ - Tìm hiểu các dịch vụ IDS/IPS - Tìm hiểu về các tập luật phát hiện xâm nhập - Tìm hiểu về các kỹ thuật trí tuệ nhân tạo dùng trong dự đoán, phát hiện xâm nhập - Lựa chọn mô hình/ thử nghiệm các thuật toán, - Phân tích dữ liệu áp dụng cho mô hình thuật toán , so sánh kết luận - Xây dựng các tình huống tấn công và thực nghiệm các phương pháp dựa trên thuật toán và mô hình đã chọn.	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT& ATTT		
11	Ứng dụng trí tuệ nhân tạo trong hệ thống IDS phát hiện xâm nhập bất thường và cảnh báo.	-Tìm hiểu các dịch vụ IDS/IPS -Ứng dụng trí tuệ nhân tạo trong việc phát hiện xâm nhập bất thường hệ thống mạng -Tìm hiểu tổng quan về trí tuệ nhân tạo và các mô hình huấn luyện. -Tìm hiểu tổng quan về hệ thống phát hiện xâm nhập (IDS) mã nguồn mở Suricata. -Tìm hiểu các tập luật phát hiện xâm nhập của Suricata -Xây dựng các tình huống tấn công mạng và thực nghiệm các phương pháp để phòng thủ bằng IDS ằng tập luật và thuật toán ứng dụng trí tuệ nhân tạo	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT& ATTT		
12	Tìm hiểu các kỹ thuật tấn công API Security, triển khai hệ thống tấn công và phòng thủ	- Tìm hiểu kiến thức về bảo mật API, Tìm hiểu các công cụ hỗ trợ trong phân tích lỗ hổng hệ thống -Phân tích lỗ hổng và lên kịch bản thực nghiệm tấn công và phòng thủ ít nhất 5 loại. □Phân tích, thiết kế, cài đặt hệ thống, hoàn chỉnh với các kỹ thuật tấn công lỗ hổng được liệt kê sau □Injection Attacks (SQL Injection, Command Injection) □Broken Authentication & Authorization □API Rate Limiting Bypass □Man-in-the-Middle (MITM) Attacks □Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF) □Server-Side Request Forgery (SSRF) □Denial-of-Service (DoS) & API Abuse □Unrestricted File Upload □IDOR (Insecure Direct Object References) □Race Condition From Code □Parameter Pollution . □Session Fixation,...	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT& ATTT		
13	Triển khai tính năng bảo mật trong xây dựng ứng dụng bán hàng điện máy	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng bán hàng điện máy có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên,ca trực, hàng hóa có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Hàng hóa có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin ca trực, hàng hóa, đặt hàng * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		

14	Triển khai tính năng bảo mật trong xây dựng ứng dụng sản xuất linh kiện ô tô	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng quản lý sản xuất linh kiện ô tô có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên,ca sản xuất, linh kiện, nguyên liệu có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Linh kiện có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin sản xuất, linh kện, đặt hàng * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		
15	Triển khai tính năng bảo mật trong xây dựng ứng dụng web mua bán ô tô	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng bán ô tô có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên,ca trực, ô tô có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Ô tô có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin ca trực, hàng hóa, đặt hàng, đặt dịch vụ lái thử * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		
16	Triển khai tính năng bảo mật trong xây dựng ứng dụng bảo dưỡng ô tô	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng bảo dưỡng ô tô có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên,ca trực, linh kiện, dịch vụ có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Linh kiện có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin ca trực, linh kiện, đặt lịch bảo dưỡng * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		

17	Triển khai tính năng bảo mật trong xây dựng ứng dụng sửa chữa và bảo hành điện thoại	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng sửa chữa và bảo hành điện thoại có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên,ca trực, linh kiện, dịch vụ có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Linh kiện có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin ca trực, linh kiện, đặt lịch sữa chữa * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		
18	Triển khai tính năng bảo mật trong xây dựng quản lý hệ thống chăm sóc vật lý trị liệu	* Triển khai trên hệ điều hành Linux, phân tích, thiết kế và cài đặt ứng dụng quản lý hệ thống chăm sóc bệnh nhân bằng vật lý trị liệu có áp dụng các tính năng bảo mật của Oracle * Các chức năng chính trên website -Quản lý kho, nhân viên, dược liệu, dịch vụ có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh + xác thực; kiểm toán - Dược liệu có có truy xuất nguồn gốc bằng mã quét QR - Quản lý theo dõi hóa đơn có lập hóa đơn được ký số - Phân quyền (kết hợp VPD, OLS) - Điều khiển truy cập MAC + DAC - Cloud database - Quản lý Tablespace, session, connection - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin dược liệu, cửa hàng, đặt lịch chăm sóc * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT& ATTT		
19	Nghiên cứu về deepfake và các giải pháp phòng chống	•Tìm hiểu công nghệ giả mạo giọng nói: Voice Cloning, AI voice synthesis •Triển khai kịch bản tấn công: gọi điện giả lãnh đạo ra lệnh chuyển tiền, giả mạo khách hàng, social engineering •Tìm hiểu các dấu hiệu nhận diện Deepfake voice: ngữ điệu, âm thanh nền, độ khớp nội dung •Tìm hiểu các biện pháp phòng chống: xác thực đa yếu tố, xác minh qua kênh song song, voice biometrics •Tìm hiểu các công cụ voice cloning để tạo giọng nói giả (môi trường offline, không phát tán). •Tìm hiểu về Deepfake video: kỹ thuật tạo bằng AI (GANs) •Mục đích tấn công: giả mạo lãnh đạo, tin giả, hạ uy tín, lừa đảo tài chính •Tìm hiểu các dấu hiệu nhận biết Deepfake: ánh sáng, chớp mắt, khớp giọng nói, biểu cảm •Tìm hiểu các công cụ phát hiện Deepfake video: oMicrosoft Video Authenticator oDeepware Scanner •Triển khai nghe và phân tích đoạn ghi âm Deepfake. •Triển khai phân tích video Deepfake mẫu, chỉ ra các chi tiết bất thường. •So sánh đoạn ghi âm, video thật với đoạn ghi âm, video Deepfake. •Kiểm tra độ tin cậy bằng công cụ AI.	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT& ATTT		
20	Xây dựng hệ thống quản lý học tập tích hợp tính năng phát hiện và nhận diện khuôn mặt (FaceID) để quản lý lớp học	Nghiên cứu, phân tích thiết kế các tính năng, xây dựng hệ thống quản lý học tập: oQuản lý giảng viên: hồ sơ giảng viên (cơ hữu và thỉnh giảng), lịch dạy, lớp dạy, v.v… oQuản lý sinh viên: hồ sơ sinh viên, lịch học, điểm số, v… oQuản lý lớp học: Tạo lớp học, điểm danh, phân nhóm, kiểm tra, điểm số, xuất danh sách điểm danh, v.v… -Xây dựng tính năng FaceID và tích hợp vào hệ thống LMS: oXử lý hình ảnh đầu vào từ camera để phục vụ cho các bước phân tích (computer vision) oXây dựng tính năng phát hiện khuôn mặt từ camera thông qua giao diện Website (object detection).	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT& ATTT		

21	Xây dựng hệ thống quản lý học tập tích hợp tính chữ ký số để quản lý và lưu chữ hồ sơ	Nghiên cứu, phân tích thiết kế các tính năng, xây dựng hệ thống quản lý học tập: oQuản lý giảng viên: hồ sơ giảng viên (cơ hữu và thỉnh giảng), lịch dạy, lớp dạy, v.v… oQuản lý sinh viên: hồ sơ sinh viên, lịch học, điểm số,.v… oQuản lý lớp học: Tạo lớp học, điểm danh, phân nhóm, kiểm tra, điểm số, xuất danh sách điểm danh, v.v… -Xây dựng tính năng chữ ký số và tích hợp vào hệ thống LMS oNghiên cứu về các hệ mã hóa ứng dụng tạo chữ ký số oXây dựng tính năng ký số trên các văn bản tích hợp vào hệ thống LMS	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT		
22	Nghiên cứu và triển khai Pentesting trên Android Applications	Kiểm tra mã nguồn, cấu hình để xem xét lỗ hổng và các hành vi bất thường bằng các kỹ thật : Phân tích tĩnh Phân tích thủ công Phân tích tự động Dịch ngược mã	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT		
23	Nghiên cứu về mã độc và ứng dụng học máy trong phát hiện mã độc	Tìm hiểu về các loại mã độc Tìm hiểu các bộ dataset về mã độc Tìm hiểu các mô hình học máy Kiểm thử mô hình xác định độ chính xác trong phát hiện mã độc	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT		
24	DỰ ĐOÁN VAI TRÒ NGƯỜI DÙNG TRÊN MẠNG XÃ HỘI BẰNG PHƯƠNG PHÁP HỌC MÁY	-Dự đoán và phân loại vai trò người dùng trên mạng xã hội, sử dụng dữ liệu định lượng từ Twitter Ego Networks. Các đặc trưng như các chỉ số Centrality (Degree, Betweenness, Eigenvector, Closeness) và thuộc tính người dùng (Num_Features) được khai thác để xây dựng tập dữ liệu đặc trưng, từ đó triển khai quy trình phân tích gồm: +Xây dựng đặc trưng phản ánh hành vi và vị trí người dùng; +Gán nhãn vai trò dựa trên ngưỡng hoặc K-means; +Mô phỏng lan truyền thông tin bằng mô hình SIR;	Vũ Đức Thịnh	thinhvd@huit.edu.vn	MMT&ATTT		
25	Xây dựng một số kịch bản khai thác lỗ hổng hệ điều hành và ứng dụng theo định danh lỗ hổng bảo mật CVE	- Nghiên cứu các lỗ hổng CVE điển hình trên hệ điều hành và ứng dụng. - Phân loại các lỗ hổng: Buffer Overflow, Command Injection, SQL Injection, RCE, Privilege Escalation... - Xây dựng các kịch bản mô phỏng khai thác lỗ hổng (trên môi trường ảo hoặc sandbox) - Xây dựng kịch bản khai thác giúp nâng cao nhận thức, khả năng phòng thủ và kiểm thử xâm nhập. - Đánh giá mức độ ảnh hưởng và biện pháp khắc phục	Lê Anh Tuấn	tuanla@huit.edu.vn	MMT&ATTT		
26	Tìm hiểu, triển khai hệ thống giám sát an ninh mạng sử dụng giải pháp mã nguồn mở LibreNMS	- Tìm hiểu kiến thức về giám sát mạng và các công cụ mã nguồn mở. - Cài đặt và triển khai hệ thống LibreNMS để giám sát mạng nội bộ (Tập trung vào chức năng giám sát mạng và phát hiện sự cố). - Đánh giá khả năng ứng dụng LibreNMS trong môi trường thực tế.	Lê Anh Tuấn	tuanla@huit.edu.vn	MMT&ATTT		
27	Nghiên cứu và phát hiện bất thường trong giao dịch Blockchain bằng Deep Learning	□Nhận diện giao dịch bất thường trong giao dịch Blockchain như rửa tiền, gian lận. □Áp dụng Graph Neural Networks (GNN) để phân tích luồng giao dịch. □Huấn luyện mô hình trên Elliptic Dataset, Ethereum Transaction Data. □Khảo sát khả năng kết hợp GNN với học tăng cường để cải thiện hiệu quả phát hiện bất thường trong đồ thị giao dịch động. □Đánh giá hiệu suất.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT		
28	Nghiên cứu thuật toán Naive Bayes kết hợp trích xuất đặc trưng ngữ nghĩa ứng dụng trong phát hiện email lừa đảo	□Phân tích các đặc trưng của email lừa đảo (Domain giả mạo, từ khoá đáng ngờ, liên kết độc hại). □Kết hợp kỹ thuật trích xuất đặc trưng ngữ nghĩa bằng BERT/Sentence-BERT để cải thiện đầu vào cho mô hình Naïve Bayes. □Thu thập tập dữ liệu email thật từ các nguồn như SpamAssassin, Enron Dataset. □Huấn luyện thuật toán Naïve Bayes để phân loại email an toàn và email lừa đảo. □Đánh giá độ chính xác của mô hình trên tập dữ liệu thực nghiệm.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT		
29	Nghiên cứu thuật toán Random Forest kết hợp trích xuất đặc trưng ngữ nghĩa ứng dụng trong phát hiện Email lừa đảo	□Phân tích các đặc trưng của email lừa đảo (Domain giả mạo, từ khoá đáng ngờ, liên kết độc hại). □Kết hợp kỹ thuật trích xuất đặc trưng ngữ nghĩa bằng BERT/Sentence-BERT để cải thiện đầu vào cho mô hình Random Forest. □Thu thập tập dữ liệu email thật từ các nguồn như SpamAssassin, Enron Dataset. □Huấn luyện thuật toán Random Forest để phân loại email an toàn và email lừa đảo. □Đánh giá độ chính xác của mô hình trên tập dữ liệu thực nghiệm.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT		
30	Nghiên cứu thuật toán XGBoost kết hợp trích xuất đặc trưng ngữ nghĩa ứng dụng trong phát hiện Email lừa đảo	□Phân tích các đặc trưng của email lừa đảo (Domain giả mạo, từ khoá đáng ngờ, liên kết độc hại). □Kết hợp kỹ thuật trích xuất đặc trưng ngữ nghĩa bằng BERT/Sentence-BERT để cải thiện đầu vào cho thuật toán XGBoost. □Thu thập và tiền xử lý tập dữ liệu email từ các nguồn công khai như SpamAssassin, Enron Corpus, Kaggle, v.v. □Xây dựng và huấn luyện thuật toán XGBoost để phát hiện Email lừa đảo. □Đánh giá mô hình dựa trên các tiêu chí: Accuracy, Precision, Recall, F1-score và ROC-AUC.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT		
31	Nghiên cứu mô hình học sâu LSTM kết hợp Word Embedding ứng dụng trong phát hiện Email lừa đảo.	□Phân tích các đặc trưng của email lừa đảo (Domain giả mạo, từ khoá đáng ngờ, liên kết độc hại). □Thu thập và tiền xử lý tập dữ liệu email từ các nguồn công khai như SpamAssassin, Enron Corpus, Kaggle, v.v. □Biểu diễn văn bản email thành dạng vector ngữ nghĩa sử dụng kỹ thuật Word Embedding (Word2Vec hoặc GloVe). □Xây dựng và huấn luyện mô hình học sâu LSTM để nhận diện email lừa đảo dựa trên dữ liệu văn bản. □Đánh giá mô hình dựa trên các tiêu chí: Accuracy, Precision, Recall, F1-score và ROC-AUC.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT		

32	Nghiên cứu thuật toán XGBoost ứng dụng trong phát hiện lưu lượng mạng bất thường.	□Phân tích hành vi truy cập mạng và xác định các đặc trưng có thể giúp nhận diện truy cập bất thường. □Thu thập và xử lý tập dữ liệu log từ nguồn công khai (CIC-IDS2017, UNSW-NB15...). □Áp dụng thuật toán XGBoost để huấn luyện mô hình phát hiện bất thường. □Kết hợp kỹ thuật xử lý dữ liệu mất cân bằng như SMOTE hoặc ADASYN để cải thiện khả năng phát hiện. □Phát triển một công cụ cảnh báo truy cập bất thường thời gian thực bằng Python (Flask/Streamlit). □Đánh giá mô hình dựa trên các tiêu chí: Accuracy, Precision, Recall, F1-score và ROC-AUC. □Đánh giá hiệu quả mô hình theo độ chính xác, độ nhạy, tốc độ xử lý.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT& ATTT		
33	Nghiên cứu và triển khai Cuckoo Sandbox	- Tìm hiểu các phần mềm Sandbox phổ biến hiện nay - Đánh giá ưu nhược điểm các Sandbox - Tìm hiểu Cuckoo sandbox - Triển khai hệ thống Cuckoo sandbox	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
34	Nghiên cứu và triển khai Detux Sandbox	- Tìm hiểu các phần mềm Sandbox phổ biến hiện nay - Đánh giá ưu nhược điểm các Sandbox - Tìm hiểu Detux sandbox - Triển khai hệ thống Detux sandbox	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
35	Nghiên cứu thuật toán học sâu thử nghiệm phát hiện tấn công từ chối dịch vụ trong IoT	- Tìm hiểu nền tảng IoT - Phân tích và lựa chọn các thuật toán phát hiện, phân loại tấn công DDoS - Nghiên cứu các thuật toán học sâu - Thực nghiệm áp dụng mô hình học sâu trong bài toán phát hiện tấn công từ chối dịch vụ IoT	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
36	Nghiên cứu thuật toán học sâu ứng dụng trong phát hiện mã độc IoT	- Tìm hiểu nền tảng IoT - Các phương pháp phát hiện mã độc IoT truyền thống và hiện đại như áp dụng mô hình học sâu - Nghiên cứu mạng thông tin hỗn tạp và mô hình đồ thị học sâu - Thực nghiệm áp dụng mạng thông tin hỗn tạp kết hợp với mô hình đồ thị học sâu trong bài toán phân lớp mã độc IoT	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
37	Nghiên cứu mạng thông tin hỗn tạp kết hợp với học máy cho bài toán phân lớp mã độc Android	- Tìm hiểu nền tảng Android - Các phương pháp phát hiện mã độc Android truyền thống và hiện đại như áp dụng mô hình học máy - Nghiên cứu mạng thông tin hỗn tạp và mô hình đồ thị học sâu - Thực nghiệm áp dụng mạng thông tin hỗn tạp kết hợp với mô hình đồ thị học sâu trong bài toán phân lớp mã độc Android.	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
38	Nghiên cứu triển khai hệ thống giám sát an ninh mạng dựa trên logfile	- Tìm hiểu các hệ thống giám sát an ninh mạng phổ biến hiện nay - Đánh giá ưu nhược điểm các hệ thống giám sát an ninh mạng phổ biến hiện nay - Thiết kế mô hình hệ thống giám sát an ninh mạng - Triển khai hệ thống giám sát an ninh mạng dựa trên logfile	Trần Đắc Tốt	tottd@huit.edu.vn	MMT& ATTT		
39	Nghiên cứu ứng dụng mạng học sâu CNN-LSTM trong phát hiện mã độc dựa trên luồng hệ thống (System Call Traces)	• Cài đặt công cụ giám sát system call như strace, sysdig hoặc auditd. • Thu thập dataset mẫu từ Cuckoo Sandbox hoặc các nguồn mã độc đã phân loại (VirusShare, VirusTotal, Malicia). • Mã hóa chuỗi system call dưới dạng one-hot hoặc word embedding. • Xây dựng mô hình học sâu kết hợp CNN-LSTM trong TensorFlow hoặc PyTorch. • So sánh mô hình CNN-LSTM với các mô hình baseline khác (SVM, CNN, LSTM riêng biệt). • Đánh giá mô hình qua các chỉ số: accuracy, precision, recall, F1-score. • Tích hợp mô hình vào demo đơn giản để người dùng nhập log và nhận kết quả phát hiện.	Hồ Hải Quân	quanhh@huit.edu.vn	MMT& ATTT		
40	Nghiên cứu phát hiện mã độc tàng hình (Fileless Malware) trong bộ nhớ bằng Deep Neural Network và kỹ thuật trích xuất đặc trưng từ RAM Dump	• Cài đặt và sử dụng công cụ forensic: Volatility hoặc Rekall để phân tích RAM Dump. • Thu thập mẫu RAM Dump có chứa hoạt động fileless malware (có thể từ môi trường sandbox). • Trích xuất đặc trưng như: command line, injected DLLs, API call, memory regions. • Tiền xử lý dữ liệu và chuyển về định dạng huấn luyện mô hình. • Huấn luyện mô hình DNN hoặc MLP với nhiều tầng ẩn. • So sánh với các mô hình truyền thống như Random Forest, SVM. • Triển khai giao diện đơn giản cho phép người dùng nhập file dump và phát hiện tiến trình nghi ngờ.	Hồ Hải Quân	quanhh@huit.edu.vn	MMT& ATTT		
41	Nghiên cứu ứng dụng mã hóa đường cong Elliptic (ECC) cho thiết bị IoT	Nghiên cứu lý thuyết về ECC và giao thức trao đổi khóa ECDH. Lựa chọn nền tảng phần cứng (ví dụ: ESP32, Raspberry Pi Pico). Triển khai trên thiết bị IoT và máy chủ Đo lường năng lượng: sử dụng thiết bị đo công suất USB (USB Power Meter) để đo dòng điện tiêu thụ của ESP32 trong quá trình mã hóa	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		
42	Nghiên cứu, phân tích an toàn của giao thức xác thực không mật khẩu FIDO2/WebAuthn	Phân rã kiến trúc FIDO2 thành các thành phần chính: Client (trình duyệt), Authenticator (khóa an ninh, Windows Hello, v.v.), và Relying Party (máy chủ web) Phân tích chi tiết hai giao thức cốt lõi: WebAuthn, CTAP (Client to Authenticator Protocol) Sơ đồ hóa các luồng dữ liệu và quá trình mật mã trong hai giao thức chính: Đăng ký (Registration Ceremony) và Xác thực (Authentication Ceremony) Xây dựng một môi trường lab hoàn chỉnh bao gồm một Relying Party mẫu Thực hiện các kịch bản tấn công giả lập để xác minh các thuộc tính an toàn. Sử dụng một thư viện FIDO2/WebAuthn mã nguồn mở để xây dựng một trang web mẫu có chức năng đăng ký và đăng nhập bằng WebAuthn Sử dụng các trình duyệt hiện đại có hỗ trợ WebAuthn (Chrome, Firefox, Edge) Sử dụng cả khóa an ninh phần cứng và trình xác thực nền tảng hực hiện Kịch bản Tấn công & Phân tích: Giả lập Phishing & MITM, Phân tích CSDL phía Server, Nghiên cứu Malware phía Client Phân tích các kết quả từ phân tích lý thuyết và thực nghiệm	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		

43	Nghiên cứu, phân tích tính an toàn của các hàm băm mật mã	Nghiên cứu sâu về các nguyên lý của mật mã học, đặc biệt là các hàm một chiều và hàm băm.. Nghiên cứu chi tiết cấu trúc và hoạt động của MD5, SHA-1, SHA-256, và SHA-3. Tấn công tìm xung đột MD5: Sử dụng các công cụ có sẵn hoặc tự triển khai một phiên bản đơn giản hóa để tạo ra hai tệp tin khác nhau nhưng có cùng một mã băm MD5 Tấn công ngày sinh: Viết chương trình mô phỏng tấn công ngày sinh để tìm ra xung đột cho một phiên bản rút gọn của một hàm băm. Mục đích là để hiểu rõ về độ phức tạp O(2n/2) của tấn công. Tạo bảng so sánh chi tiết các hàm băm dựa trên các tiêu chí: độ dài đầu ra, kích thước khối, cấu trúc, mức độ an toàn lý thuyết và khả năng chống lại các loại tấn công đã biết Phân tích kết quả từ giai đoạn thực nghiệm: thời gian tạo xung đột, tài nguyên cần thiết	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		
44	Nghiên cứu phát hiện tấn công xen giữa (Man-in-the-Middle) qua phân tích chứng chỉ số	Tìm hiểu sâu về giao thức TLS/SSL, đặc biệt là quá trình bắt tay (handshake). Nghiên cứu cấu trúc của chứng chỉ số X.509 và các trường thông tin quan trọng. Phân loại các kỹ thuật tấn công MITM liên quan đến chứng chỉ: SSL Stripping, DNS Spoofing kết hợp với chứng chỉ giả mạo, tấn công sử dụng CA giả mạo. Nghiên cứu các công cụ mã nguồn mở dùng để thực hiện tấn công MITM Thiết lập môi trường mạng ảo hóa (sử dụng VirtualBox hoặc VMware) với các máy ảo Lựa chọn ngôn ngữ lập trình (Python) và các thư viện cần thiết (Scapy hoặc pyshark để bắt gói tin, cryptography hoặc pyOpenSSL để phân tích chứng chỉ). Viết mã cho Thành phần thu thập dữ liệu: Sử dụng thư viện đã chọn để lọc các gói tin TLS/SSL và trích xuất dữ liệu chứng chỉ. Viết mã cho Thành phần phân tích, Thành phần cảnh báo: In ra console, ghi vào file log, hoặc gửi thông bá Thực hiện các kịch bản tấn công MITM trong môi trường ảo hóa Đánh giá độ chính xác (True Positive, False Positive) của công cụ và tinh chỉnh lại các quy tắc nếu cần	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		
45	Nghiên cứu so sánh các giao thức trao đổi khóa Diffie-Hellman và Elliptic Curve Diffie-Hellman (ECDH)	Tìm hiểu sâu về lý thuyết nhóm, trường hữu hạn và nền tảng toán học của Diffie-Hellman truyền thống. Nghiên cứu toán học đường cong Elliptic trên trường hữu hạn Phân tích chi tiết thuật toán trao đổi khóa DH và ECDH từng bước Nghiên cứu các thuật toán tấn công hiệu quả nhất cho DLP (như General Number Field Sieve - GNFS) và cho ECDLP (như thuật toán Pollard's rho, Pohlig-Hellman). So sánh độ phức tạp của chúng Thiết kế và viết chương trình benchmark Thực thi chương trình benchmark cho DH với các kích thước khóa phổ biến: 2048-bit, 3072-bit Thực thi chương trình benchmark cho ECDH với các đường cong cung cấp mức an toàn tương đương: secp224r1, secp256r1 (tương đương DH 2048/3072-bit) Tạo các biểu đồ so sánh hiệu năng (tốc độ theo mức an toàn, kích thước khóa theo mức an toàn). Phân tích và diễn giải kết quả, chỉ ra sự khác biệt rõ rệt về hiệu năng và chi phí tài nguyên.	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		
46	Nghiên cứu và triển khai thuật toán mã hóa kháng lượng tử (Post-Quantum Cryptography - PQC)	Tìm hiểu về máy tính lượng tử và thuật toán Shor, chứng minh tại sao nó có thể phá vỡ RSA/ECC. Nghiên cứu tổng quan về cuộc thi tiêu chuẩn hóa PQC của NIST: các vòng thi, các nhóm thuật toán, và các thuật toán chiến thắng Chọn một thuật toán cụ thể (CRYSTALS-Kyber) hoặc tương tự và đi sâu vào bài báo gốc mô tả nó. Phân tích chi tiết các bước: tạo khóa (KeyGen), đóng gói (Encapsulate), và mở gói (Decapsulate) ìm hiểu và cài đặt thư viện liboqs (Open Quantum Safe). Đây là một thư viện mã nguồn mở cung cấp các bản triển khai tham khảo của nhiều thuật toán PQC Viết các chương trình "hello-world" đơn giản để đảm bảo đã tích hợp thư viện thành công và có thể gọi các hàm API cơ bản của Kyber/Dilithium Lập trình ứng dụng benchmark theo mô hình đã xác định đối với Kyber (KEM): đo thời gian crypto_kem_keypair() (tạo cặp khóa), đo thời gian crypto_kem_enc() (tạo khóa chung và bản mã), đo thời gian crypto_kem_dec() (giải mã để lấy khóa chung), ghi nhận kích thước khóa công khai, khóa bí mật và bản mã Lập trình ứng dụng benchmark theo mô hình đã xác định đối với Dilithium (Signature): đo thời gian crypto_sign_keypair() (tạo cặp khóa), đo thời gian crypto_sign() (ký lên thông điệp), đo thời gian crypto_sign_open() (xác thực chữ ký), ghi nhận kích thước khóa công khai, khóa bí mật và chữ ký Tổng hợp dữ liệu vào bảng và vẽ biểu đồ so sánh (ví dụ: biểu đồ cột so sánh thời gian, kích thước khóa) Phân tích các sự đánh đổi (trade-offs) của PQC so với mã hóa truyền thống	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT& ATTT		

KT. TRƯỞNG KHOA

Nguyễn Thanh Long

NGƯỜI LẬP BIỂU

Lương Thị Quỳnh Mai