MỘT SỐ ĐỀ TÀI TIỂU LUẬN AN NINH MẠNG

STT	Tên đề tài	Yêu cầu chung
1	Tìm hiểu và triển khai IPSec VPN với phần mềm giả lập GNS3	***Lý thuyết:*** - Tìm hiểu hoạt động của giao thức IPSec - Tìm hiểu về VPN: Khái niệm và các mô hình triển khai ***Thực hành:*** - Cài đặt phần mềm giả lập GNS3 - Triển khai thử nghiệm IPSec VPN trên GNS3 theo 2 mô hình site-to-site và client-to-site (Remote Access).
2	Tìm hiểu hệ thống PKI và triển khai thử nghiệm	***Lý thuyết:*** - Tìm hiểu khái niệm và các thành phần của PKI - Tìm hiểu các kiến trúc PKI - Tìm hiểu về chứng thư số X.509 ***Thực hành:*** - Cài đặt hệ thống PKI EJBCA theo kiến trúc Single CA - Thử nghiệm các tính năng của EJBCA để cấp phát, chứng thực, quản lý, thu hồi chứng thư số
3	Tìm hiểu giao thức OAuth và xây dựng ứng dụng thử nghiệm	***Lý thuyết:*** - Tìm hiểu khái niệm và hoạt động của giao thức OAuth 1.0 và OAuth 2.0 ***Thực hành:*** - Xây dựng ứng dụng Web sử dụng giao thức OAuth để chia sẻ quyền truy cập
4	Tìm hiểu giải pháp One-TimePassword và xây dựng ứng dụng thử nghiệm	***Lý thuyết:*** - Tìm hiểu khái niệm và mô hình sử dụng OTP - Tìm hiểu các thuật toán sinh OTP: HOTP và TOTP ***Thực hành:*** - Xây dựng ứng dụng có mô-đun tạo và xác thực OTP, mô-đun đăng nhập sử dụng OTP.
5	Tìm hiểu các kỹ thuật tấn công giả mạo thông tin trong dịch vụ DNS và triển khai DNSSEC để phòng chống	***Lý thuyết:*** - Tìm hiểu các kỹ thuật tấn công DNS Spoofing và DNS Cache Poisoning ***Thực hành:*** - Thử nghiệm các kịch bản tấn công, giả định kẻ tấn công nằm trong cùng mạng LAN với nạn nhân - Triển khai thử nghiệm DNSSEC để phòng chống tấn công

6	Xây dựng Website thử nghiệm khai thác lỗ hổng Web và cách thức phòng chống	***Lý thuyết:*** - Tìm hiểu về các lỗ hổng ứng dụng Web: SQL Injection, XSS, CSRF - Tìm hiểu các kỹ thuật lập trình an toàn để phòng tránh các lỗ hổng trên ***Thực hành:*** Xây dựng Website gồm có 2 phiên bản: - Phiên bản 1: Có các lỗ hổng để minh họa các kịch bản tấn công - Phiên bản 2: Sử dụng các kỹ thuật lập trình an toàn để vá các lỗ hổng trên.
7	Tìm hiểu về hệ thống tường lửa(firewall) và triển khai thử nghiệm	***Lý thuyết:*** - Tìm hiểu về khái niệm tường lửa và các mô hình triển khai - Tìm hiểu các công nghệ tường lửa ***Thực hành:*** -Triển khai thử nghiệm tường lửa trên một mạng mô phỏng để bảo vệ cho Web Server sử dụng Mod Security và một giải pháp tường lửa mức mạng bất kỳ. -Thực hiện các kịch bản thử nghiệm.
8	Tìm hiểu các kỹ thuật tấn công Clickjacking trên dịch vụ Web và thử nghiệm các cách thức phòng chống	***Lý thuyết:*** - Tìm hiểu khái niệm tấn công Clickjacking - Tìm hiểu các kỹ thuật tấn công Clickjacking - Tìm hiểu các cách thức phòng chống ***Thực hành:*** - Thử nghiệm các kỹ thuật tấn công Clickjacking - Thử nghiệm các biện pháp phòng chống
9	Tìm hiểu tấn công DoS/DDoS trong mạng và cách thức phòng chống	***Lý thuyết:*** - Tìm hiểu khái niệm tấn công DoS/DDoS - Tìm hiệu một số kỹ thuật tấn công DoS trong mạng: Ping of Death, Teardrop, TCP SYN Flood, DNS Amplification Attack - Tìm hiểu các cách thức phòng chống những kỹ thuật tấn công trên ***Thực hành:*** - Thử nghiệm và phân tích đặc điểm của các kỹ thuật tấn công - Thử nghiệm một số cách thức phòng chống các kỹ thuật tấn công

10	Tìm hiểu các kỹ thuật tấn công DoS/DDoS tại tầng ứng dụng và cách thức phòng chống	***Lý thuyết:*** - Tìm hiểu các kỹ thuật tấn công DoS/DDoS Layer 7 vào Website - Tìm hiểu các cách thức phòng chống DoS/DDoS Layer 7 ***Thực hành:*** - Triển khai ít nhất 02 giải pháp phòng chống DoS/DDoS Layer 7 cho Website - Thực hiện các kịch bản thử nghiệm
11	ARP Spoofing & MITM	***Lý thuyết:*** - Hiểu cơ chế hoạt động của ARP. - Thực hiện ARP Poisoning trong mạng LAN (lab ảo). - Bắt và phân tích gói tin bị chuyển hướng (Wireshark). - Đánh giá rủi ro và đưa ra biện pháp phòng chống.
12	SQL Injection (DVWA)	***Lý thuyết:*** - Hiểu cơ chế SQL Injection và dạng lỗi phổ biến. - Thực hiện login bypass đơn giản. - Khai thác union-based hoặc error-based. - Phân tích nguyên nhân và đề xuất giải pháp (Prepared Statement).
13	XSS (Stored & Reflected)	***Lý thuyết:*** - Tìm hiểu nguyên lý XSS. - Thực hành tạo payload alert(), cookie stealing. - So sánh stored vs reflected XSS. - Đưa ra các phương pháp phòng chống: input sanitize, CSP.
14	Phân tích TCP Handshake bằng Wireshark	***Lý thuyết:*** - Bắt gói tin TCP khi truy cập website. - Xác định SYN, SYN/ACK, ACK. - Phân tích các flag, sequence number. - Giải thích vai trò handshake trong bảo mật.
15	Hardening Windows	***Lý thuyết:*** - Tìm và tắt các service không cần thiết. - Cấu hình firewall rule cơ bản. - Kích hoạt audit logs cần thiết. - Đưa ra checklist bảo mật Windows.
16	Logging & giám sát sự kiện Windows	***Lý thuyết:*** - Bật Audit Log đầy đủ. - Thu thập log về login fail/success. - Phân tích event ID 4624, 4625, 4672. - Mô phỏng brute-force và phân tích dấu vết.

17	Bảo mật API với JWT	***Lý thuyết:*** - Giải thích cấu trúc JWT (header.payload.signature). - Tạo API login sinh token. - Thử sửa payload → signature sai. - Test expired token & replay. - Đề xuất bảo vệ: TTL ngắn, rotate token.
18	Phân tích Email Phishing	***Lý thuyết:*** - Thu thập một email scam. - Phân tích header: Received-from, SPF, DKIM. - Nhận diện dấu hiệu lừa đảo. - Đề xuất cách phòng tránh.
19	Wi-Fi Security – WPA2 Handshake	***Lý thuyết:*** - Tìm hiểu cơ chế 4-way handshake. - Bắt handshake bằng airodump-ng. - Phân tích handshake trong Wireshark. - Đánh giá điểm mạnh/yếu WPA2
20	Dò tìm host bằng Nmap	***Lý thuyết:*** - Scan port, detect OS. - Xác định service version. - Thử scan stealth (SYN scan). - Đánh giá rủi ro từ port mở.
21	Footprinting – DNS & Whois	***Lý thuyết:*** - Thu thập thông tin domain: NS, MX, A. - Tra cứu thông tin chủ sở hữu bằng Whois. - Phân tích cấu trúc tổ chức domain. - Đánh giá lộ lọt thông tin từ domain.
22	Social Engineering	***Lý thuyết:*** - Tìm hiểu các hình thức tấn công: phishing, baiting, vishing. - Sưu tầm ví dụ thực tế tại Việt Nam. - Phân tích yếu tố tâm lý bị khai thác. - Đề xuất biện pháp giáo dục người dùng.
23	Phân tích file PE	***Lý thuyết:*** - Giải thích cấu trúc PE: DOS header, NT header, section. - Dùng CFF Explorer xem import table. - Phân tích hành vi cơ bản của file. - Ứng dụng trong phát hiện malware.
24	HTTP/HTTPS Interception bằng mitmproxy	***Lý thuyết:*** - Cấu hình proxy cho trình duyệt. - Bắt HTTP/HTTPS traffic. - Phân tích cookie, headers, body. - Rút ra cách HTTPS bảo vệ dữ liệu.