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 giải pháp Single-Sign-On và xây dựng ứng dụng thử nghiệm	Lý thuyết: - Tìm hiểu khái niệm và nguyên lý hoạt động của giải pháp Single Sign On - Tìm hiểu các giải pháp Single Sign On phổ biến: OpenID Connect, SAML, CAS, JOSSO Thực hành: - Xây dựng tính năng đăng nhập cho một Website sử dụng Single Sign On.
4	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
5	Tìm hiểu giải pháp One-Time-Password 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.

6	Xây dựng ứng dụng sử dụng chữ ký số xác thực văn bản điện tử	Xây dựng ứng dụng chia sẻ và quản lý tài liệu theo mô hình client-server Server có các chức năng sau: - Cho phép người dùng tạo nhóm. Người tạo nhóm có quyền trưởng nhóm - Mỗi nhóm có một thư mục riêng, chứa các file được chia sẻ trong nhóm đó - Cho thành viên bất kỳ trong nhóm cũng có thể upload file, tạo thư mục con trong thư mục của nhóm đó - Chỉ có trưởng nhóm có quyền xóa file, thư mục con Client có các chức năng sau: - Tạo nhóm chia sẻ. - Xin tham gia một nhóm - Upload file. Trên file được upload phải có chữ ký số của người upload - Download file. Sau khi download, người dùng có thể kiểm tra chữ ký số trên file có hợp lệ không -Nếu người dùng là trưởng nhóm có thêm các quyền đã mô tả như trên
7	Xây dựng ứng dụng truyền tin bảo mật trong mạng cục bộ	Xây dựng ứng dụng theo mô hình client-server - Người dùng phải đăng ký, đăng nhập để sử dụng dịch vụ - Khi 1 user kết nối tới, cung cấp danh sách các user khác đang online - Chuyển lời mời giữa các user - Các user có thể gửi file cho nhau - Khi có 1 trong 2 user ngắt kết nối hoặc yêu cầu dừng cuộc trò chuyện, thông báo cho bên còn lại biết. - Cho phép user chuyển sang cuộc trò chuyện khác (với user khác nếu cần)
8	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

9	Tìm hiểu một số dạng tấn công trong mạng và thử nghiệm	Lý thuyết: - Tìm hiểu chi tiết các dạng tấn công ARP Poisoning, DHCP Spoofing, MAC Flooding, TCP Injection - Tìm hiểu các giải pháp phòng chống tấn công Thực hành: - Thử nghiệm các kịch bản tấn công trong môi trường mạng LAN và phân tích đặc điểm của các kỹ thuật tấn công - Thử nghiệm các kỹ thuật phòng chống tấn công
10	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
11	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
12	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. - Xây dựng

13	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
14	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.
15	Tìm hiểu về hệ thống phát hiện xâm nhập Snort hoặc Suricata	Lý thuyết: - Tìm hiểu khái niệm chung về IDS - Tìm hiểu về các thành phần kiến trúc và hoạt động của Snort (Suricata) - Tìm hiểu về cú pháp của luật trong Snort (Suricata) Thực hành: - Cài đặt hệ thống Snort (Suricata) để phát hiện xâm nhập mạng - Viết các luật Snort (Suricata) để phát hiện các tấn công dạng quét mạng, quét cổng dịch vụ, tấn công SQL Injection, XSS và các dạng tấn công khác theo ý tưởng của sinh viên. -Thực hiện các kịch bản thử nghiệm.