Dưới đây là danh sách các chủ đề nghiên cứu tiềm năng liên quan đến bảo mật, hacking và mạng máy tính, được phân loại theo lĩnh vực để bạn dễ dàng tham khảo:

1. Bảo mật mạng

Đánh giá và cải thiện an ninh trong mạng 5G.

Các chiến lược phòng thủ trước tấn công DDoS trong thời gian thực.

Phân tích hành vi bất thường trong mạng bằng Machine Learning.

Ứng dụng trí tuệ nhân tạo để phát hiện tấn công zero-day.

Bảo mật mạng không dây Wi-Fi 6 trước các cuộc tấn công Evil Twin.

Phát triển hệ thống phát hiện và ngăn chặn xâm nhập mạng (IDS/IPS) hiệu quả hơn.

Tấn công và bảo mật trong giao thức mạng IPv6.

Mô phỏng các phương pháp tấn công trong môi trường mạng doanh nghiệp (Penetration Testing).

Ứng dụng blockchain trong bảo mật giao thức mạng ngang hàng (P2P).

2. Hacking và bảo mật ứng dụng web

Tìm hiểu và khai thác các lỗ hổng OWASP Top 10 (XSS, SQL Injection, CSRF).

Phát triển công cụ quét lỗ hổng tự động cho ứng dụng web.

Nghiên cứu bảo mật API RESTful và GraphQL.

Tấn công và phòng thủ tấn công brute force vào hệ thống xác thực.

Phân tích và giảm thiểu rủi ro từ tấn công DNS Spoofing.

Sử dụng sandbox để cô lập các cuộc tấn công mã độc trên trình duyệt web.

Đánh giá bảo mật các nền tảng thương mại điện tử.

3. Bảo mật hệ thống IoT (Internet of Things)

Nghiên cứu các phương pháp bảo mật trong IoT y tế (ví dụ: máy theo dõi sức khỏe).

Phòng chống tấn công Botnet trên các thiết bị IoT.

Phân tích các lỗ hổng trong giao thức MQTT của IoT.

Mô phỏng và ngăn chặn tấn công Man-in-the-Middle trên thiết bị IoT.

Bảo mật hệ thống nhà thông minh trước các cuộc tấn công mạng.

Đề xuất cơ chế mã hóa nhẹ cho thiết bị IoT có tài nguyên hạn chế.

4. Mật mã học và bảo vệ dữ liệu

Phân tích tính an toàn của thuật toán mã hóa lượng tử (Quantum Cryptography).

Ứng dụng mã hóa đồng hình (Homomorphic Encryption) trong bảo vệ dữ liệu.

So sánh hiệu quả giữa các thuật toán mã hóa truyền thống (RSA, AES, ECC).

Phân tích các phương pháp tấn công brute force và cách tăng cường bảo mật mật khẩu.

Thiết kế hệ thống xác thực đa yếu tố (MFA) dựa trên sinh trắc học.

Bảo mật dữ liệu cá nhân bằng chữ ký số trong giao dịch trực tuyến.

5. Bảo mật trong điện toán đám mây

Phòng chống tấn công chiếm quyền điều khiển (Account Hijacking) trên nền tảng đám mây.

Đánh giá các công cụ mã hóa để bảo vệ dữ liệu trên đám mây.

Phân tích bảo mật trong container (Docker, Kubernetes).

Phát hiện và xử lý tấn công nội bộ (Insider Threats) trong môi trường đám mây.

Ứng dụng Zero Trust Architecture để bảo mật các dịch vụ đám mây.

6. Ứng dụng AI và Machine Learning trong bảo mật

Phát hiện mã độc (malware detection) bằng các mô hình học sâu (Deep Learning).

Tăng cường bảo mật mạng bằng AI tự học thích ứng với các cuộc tấn công mới.

Ứng dụng AI để phát hiện và ngăn chặn email phishing.

Đánh giá tính an toàn của các mô hình AI trước các tấn công giả mạo (Adversarial Attacks).

Tối ưu hóa hệ thống phát hiện xâm nhập (IDS) bằng học máy.

7. Phân tích mã độc (Malware Analysis)

Kỹ thuật đảo ngược mã độc (Reverse Engineering) và phân tích hành vi.

Tạo môi trường giả lập (sandbox) để theo dõi hoạt động của mã độc.

Phân tích ransomware và cơ chế mã hóa của nó.

Nghiên cứu cách thức phát tán của virus máy tính và các biện pháp phòng ngừa.

Đánh giá công cụ bảo mật (antivirus) phổ biến với các loại mã độc mới.

8. Các chủ đề khác liên quan đến bảo mật

Đánh giá bảo mật hệ thống SCADA trong các ngành công nghiệp.

Nghiên cứu bảo mật cho mạng lưới blockchain và hợp đồng thông minh (smart contracts).

Tìm hiểu các kỹ thuật Social Engineering trong hacking và cách phòng ngừa.

Bảo mật hệ thống máy ATM trước các cuộc tấn công skimming.

Xây dựng honeypot để nghiên cứu hành vi của hacker.