MÔN BẢO MẬT MẠNG

Đề tài: Phát hiện và ngăn ngừa Ransomware trong mạng doanh nghiệp & SMB

Vấn đề.

- Là mối đe doạ lớn nhất cho cả doanh nghiệp lớn và SMB (Small/Medium Business). Theo Verizon DBIR 2025, ransomware chiếm 75% các vụ xâm nhập hệ thống, SMB bị ảnh hưởng nặng nề.
- Tầm quan trọng: Khi ransomeware lây lan, dẫn đến toàn bộ dữ liệu doanh nghiệp bị mã hoá, hệ thống gián đoạn gây tổn thất và mất uy tín cho doanh nghiệp. SMB sẽ khó khăn do không có đội ngũ bảo mật chuyên môn.

Kế hoạch thực hiện

1. Tuần 1-2:
    - Thu thập các báo cáo mới về ransomeware, thực trạng, mức độ tổn thất khi bị tấn công, các lỗ hổng khai thác thường gặp, các phương pháp phòng thủ.
    - Soạn phần tổng quan về Ransomeware, các khái niệm, phương pháp, vấn đề, thực tế trong báo cáo.
2. Tuần 2-5:
    - Xây dựng Demo lab. Cài đặt môi trường máy ảo phù hợp: 1 máy chủ làm nơi backup, 1 máy nạn nhân, 1 máy attacker.
    - Tạo script ransomeware để mã hoá
    - Cài đặt và cấu hình công cụ giám sát
    - Tạo kịch bản demo: gồm 3-4 kịch bản để thực hiện việc so sánh kết quả:
        - Không có phòng thủ: toàn bộ bị mã hoá
        - Có IDS/IPS: phát hiện và chặn gói tin gây hại
        - Có backup offline: để khôi phục dữ liệu
3. Tuần 6:
    - Slide và thuyết trình.
    - Chốt báo cáo word.

Tiến độ làm việc của các thành viên

Họ và Tên	Công việc	Tiến độ hoàn thành
Lê Hoàng Phúc Thịnh	Trình bày phương pháp phòng thủ quản trị, viết script mã độc ransomware, làm slide, làm Latex	100%
Nguyễn Hải Đăng	Trình bày chương 2, phương pháp phòng thủ truyền thống, thực hiện demo backup bằng công cụ QuadStor, làm Latex	100%
Võ Thị Lan Chi	Trình bày chương 1, phương pháp phòng thủ nâng cao, thực hiện demo phát hiện bằng công cụ Suricata, làm slide, làm Latex	100%