Module 1: Tổng quan

An toàn thông tin là công cuộc bảo vệ các nhân, tổ chức, chính phủ khỏi những cuộc tấn công công nghệ bằng cách bảo vệ hệ thống mạng và dữ liệu.
Ba loại bảo vệ: cá nhân, tổ chức, chính phủ
Khối McCumber:

- Bộ ba CIA: Tính bí mật, tính toàn vẹn, tính sẵn sàng
- 3 trạng thái thông tin: đang xử lý, đã lưu, đang vận chuyển
- Biện pháp bảo mật: huấn luyện người dùng, các thiết bị công nghệ, chính sách và thủ tục

Các loại attacker: script kiddies, hacker lẻ, hackers có tổ chức
2 mối đe dọa: trong (nhân viên, đối tác) và ngoài (những kẻ tấn công ngoài tổ chức)
Chiến tranh mạng: dùng công nghệ để tấn công hệ thống máy tính nước khác để phá hoại cơ sở hạ tầng hoặc ăn cắp bí mất quốc gia.

Module 2: Các tấn công

2.1. Mã độc

Những loại mã dùng để trộm dữ liệu, trốn kiểm soát truy cập hoặc gây hại cho hệ thống.
VD: Spyware (phần mềm gián điệp), adware (quảng cáo), backdoor (cổng sau), ransomware (tống tiền), rootkit, virus, trojan horse (giả vờ là ứng dụng khác), worm (tự nhân bản)
Triệu chứng: tăng lượng tiêu thụ CPU, máy đơ hoặc hay crash, giảm tốc độ mạng, các biểu tượng lạ trên desktop, các chương trình lạ chạy trong nền

2.2. Phương pháp tấn công

Tấn công phi kỹ thuật: giả mạo danh tính, bám đuôi qua hệ thống an ninh
DoS/DDoS: làm gián đoạn hệ thống mạng bằng cách gửi quá nhiều gói tin / gửi gói tin độc.
Cach ngan chan DDoS/Botnet

Botnet: mạng lưới máy tính bị kiểm soát bởi kẻ tấn công, thường dùng để DDoS, spam email hoặc vét mật khẩu
MitM: chặn bắt kết nối giữa 2 thiết bị
Đầu độc SEO: đưa các trang web giả mạo lên đầu thanh tìm kiếm
Crack mật khẩu: từ điển, vét, cầu vồng
Tấn công có chủ đích:

Module 3:

Module 4:

Module 5:

Tên các anh cùng bàn:
Du 95
Hoàng Anh 98
Anh áo xanh gần cửa vừa nãy chưa nghe rõ 😕
Thắng ??
Minh 96
Phú 89