

VIDEO 1 :

1. Wi-Fi Password Cracking – Quá trình khám phá mật khẩu

- **Kỹ thuật xã hội (Social engineering)** – Kẻ tấn công thao túng một người biết mật khẩu để khiến họ tiết lộ mật khẩu đó.
- **Tấn công vét cạn (Brute-force attacks)** – Kẻ tấn công thử nhiều mật khẩu có thể có để đoán ra mật khẩu đúng.
- **Nghe lén mạng (Network sniffing)** – Mật khẩu có thể bị phát hiện bằng cách nghe và thu thập các gói tin được gửi trên mạng.

2. Lừa đảo trực tuyến (Phishing)

- **Phishing (Lừa đảo qua mạng):**
 - Kẻ tấn công gửi email giả mạo, trông như đến từ một nguồn hợp pháp hoặc đáng tin cậy.
 - Mục đích là lừa người nhận cài đặt phần mềm độc hại lên thiết bị của họ hoặc chia sẻ thông tin cá nhân/tài chính.
- **Spear phishing (Lừa đảo nhắm mục tiêu cụ thể):**
 - Là hình thức lừa đảo được nhắm đến một cá nhân hoặc tổ chức cụ thể, với mức độ tinh vi và chính xác cao hơn.

3. Khai thác lỗ hổng bảo mật (Vulnerability Exploitation)

- **Khai thác lỗ hổng bảo mật** – quét để tìm lỗ hổng có thể khai thác

Bước 1: Thu thập thông tin về hệ thống mục tiêu bằng cách sử dụng trình quét cổng (port scanner) hoặc kỹ thuật xã hội (social engineering)

Bước 2: Phân tích và xác định thông tin đã thu được từ bước 1

Bước 3: Tìm kiếm lỗ hổng bảo mật

Bước 4: Sử dụng mã khai thác (exploit) có sẵn hoặc viết mã khai thác mới

- **Mối đe dọa dai dẳng nâng cao (Advanced Persistent Threats - APT)** – là một hoạt động tấn công nhiều giai đoạn, dài hạn, bí mật và tinh vi nhằm vào một mục tiêu cụ thể
 - Thường được tài trợ tốt
 - Triển khai phần mềm độc hại tùy chỉnh

Video 2:

Phương pháp xâm nhập (Methods of Infiltration)

“Kỹ thuật xã hội (Social Engineering)”

- *Kỹ thuật xã hội – là việc lừa thao túng con người để họ thực hiện hành động hoặc tiết lộ thông tin bí mật.”*
 - Giả danh (Pretexting) – kẻ tấn công gọi điện hoặc tiếp cận nạn nhân và nói dối nhằm giành quyền truy cập vào dữ liệu quan trọng.
 - Đi theo sau (Tailgating) – kẻ tấn công nhanh chóng đi theo một người được ủy quyền để vào khu vực an toàn.
 - Trao đổi có điều kiện (Something for something – Quid pro quo) – kẻ tấn công yêu cầu thông tin cá nhân của nạn nhân để đổi lấy một lợi ích nào đó.