# Module 2: Footprinting and Reconnaissance

## Khái niệm cơ bản

Footprinting là bướ đầu tiên trong hack có đạo đức, là giai đoạn chuẩn bị trước khi tấn công, kẻ tấn công thu thập càng nhiều thông tin càng tốt để dễ dàng tìm cách xâm nhập vào mạng mục tiêu

Footprinting là xác định mức độ rủi ro liên quan đến thông tin công khai của tổ chức.

Thông tin thu thập được:

-Thông tin về tổ chức: Thông tin về nhân viên, đối tác, web, báo, …

-Thông tin về mạng: Tên miền, network block, ip, cấu trúc liên kết, …

-Thông tin về hệ thống: Hệ điều hành của web server, vị trí của server, …

Mục đích:

-Biết sơ đồ an ninh của tổ chức

-Xác định được các điểm yếu

-Vẽ sơ đồ mạng

## Phân loại

2 loại:

-Thụ động:

Footprinting thụ động liên quan đến việc thu thập thông tin về mục tiêu mà không cần tương tác trực tiếp do đó không bị mục tiêu phát hiện.

Về mặt kỹ thuật, thực hiện rất khó

Các kỹ thuật:

+Tìm kiếm thông tin thông qua công cụ tìm kiếm

+Tìm miền cấp cao nhất (TLD) và miền phụ của mục tiêu

+Tìm vị trí thông qua dịch vụ web

+Tìm kiếm người thông qua trang mạng xã hội

….

-Chủ động:

Footprinting chủ động liên quan đến việc thu thập thông tin về mục tiêu với sự tương tác trực tiếp.

Mục tiêu có thể nhận ra quá trình thu thập thông tin đang diễn ra

Footprinting đòi hỏi sự chuẩn bị nhiều hơn vì để lại dấu vết

Kỹ thuật:

+Tìm kiếm file

+Trích xuất liên kết trang web và thu thập danh sách

+Trích xuất siêu dữ liệu

+Thu thập thông tin thông qua theo dõi email

+Tra cứu Whois

+Trích xuất thông tin DNS

## Phương pháp thu thập thông tin

### Thu thập thông tin bằng công cụ kìm tiếm

a. Advanced Google

## Kỹ thuật tấn công thăm dò

## Dò quét lỗ hổng bảo mật

## Kỹ thuật liệt kê

## Giair pháp phòng chống