

## Bài: 2.1 Dấu vết & Thăm dò - Khái niệm & Mục tiêu của việc thăm dò dấu vết

Xem bài học trên website để ủng hộ Kteam: [2.1 Dấu vết & Thăm dò - Khái niệm & Mục tiêu của việc thăm dò dấu vết](#)

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage [How Kteam](#) nhé!

### Công nghệ tóm tắt

Kẻ tấn công sẽ nhắm tới mục đích khi **Footprinting phase** cho phép hân thu thập thông tin về kiến trúc an ninh trong nội bộ và cả bên ngoài. Việc sưu tập thông tin cũng giúp xác định các lỗ hổng trong một hệ thống, những thứ khai thác, để truy cập.

Tiếp nhận thông tin sâu về mục tiêu là giảm đi những điểm trọng tâm và đưa kẻ tấn công đến gần mục tiêu hơn. Kẻ tấn công sẽ tập chung vào mục tiêu bằng địa chỉ IP mà hân kiểm tra, để tấn công mục tiêu hoặc liên quan đến những thông tin tên miền hay những thứ khác.

### Khái niệm của việc dò tìm dấu vết

Bước đầu tiên để “hack” có thiện chí là việc **dò tìm dấu vết**.

Dò tìm dấu vết là sự thu thập mọi thông tin có thể có liên quan đến mục tiêu và mạng mục tiêu. Bộ sưu tập thông tin này giúp xác định các cách khác nhau để tham gia vào mạng mục tiêu. Bộ sưu tập thông tin này có thể đã thu thập được thông qua thông tin cá nhân có sẵn công khai & thông tin nhạy cảm từ bất cứ nguồn bí mật nào.

Thông thường, việc dò tìm dấu vết và thăm dò đang thực hiện các cuộc tấn công xã hội, tấn công hệ thống hay tấn công mạng hoặc thông qua bất kỳ kỹ thuật nào khác. Các phương thức thăm dò chủ động hay bị động cũng đều phổ biến để thu thập thông tin về mục tiêu theo cách trực tiếp hoặc gián tiếp.

Mục đích chung của giai đoạn này là giữ được tương tác với mục tiêu để thu được những thông tin mà không có bất kỳ phát hiện hay cảnh báo nào xảy ra.

### Thăm dò dấu vết giả mạo(Pseudonymous Footpringting)

**Thăm dò dấu vết giả mạo** bao gồm cả những dấu vết thông qua các nguồn trực tuyến. Trong dấu vết thăm dò giả mạo đó, thông tin về mục tiêu được chia sẻ bằng cách đăng với một tên giả định. ID loại thông tin này được chia sẻ với thông tin xác thực để tránh sự theo dõi đến một nguồn thông tin thực khác.

### Thăm dò dấu vết mạng (Internet Footprinting)

**Thăm dò dấu vết mạng** bao gồm các cách dò lần hay thăm dò để thu thập thông tin thông qua mạng. Trong việc thăm dò dấu vết mạng, quá trình như Google Hacking, Google Search, Google Application và bao gồm cả những công cụ tìm kiếm khác ngoài Google.

### Mục tiêu của việc thăm dò dấu vết

Những mục tiêu chính của việc thăm dò dấu vết đó là:

1. Để biết đặc điểm bảo mật
2. Để giảm thiểu vùng trọng tâm
3. Để xác định những lỗ hổng
4. Vẽ bản đồ mạng

