Bài: 2.2 Dấu vết & Thăm dò - Cách thăm dò dấu vết (Phần 1)

Xem bài học trên website để ủng hộ Kteam: 2.2 Dấu vết & Thăm dò - Cách thăm dò dấu vết (Phần 1)

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!

Cách thăm dò dấu vết (Footprinting Methodology)

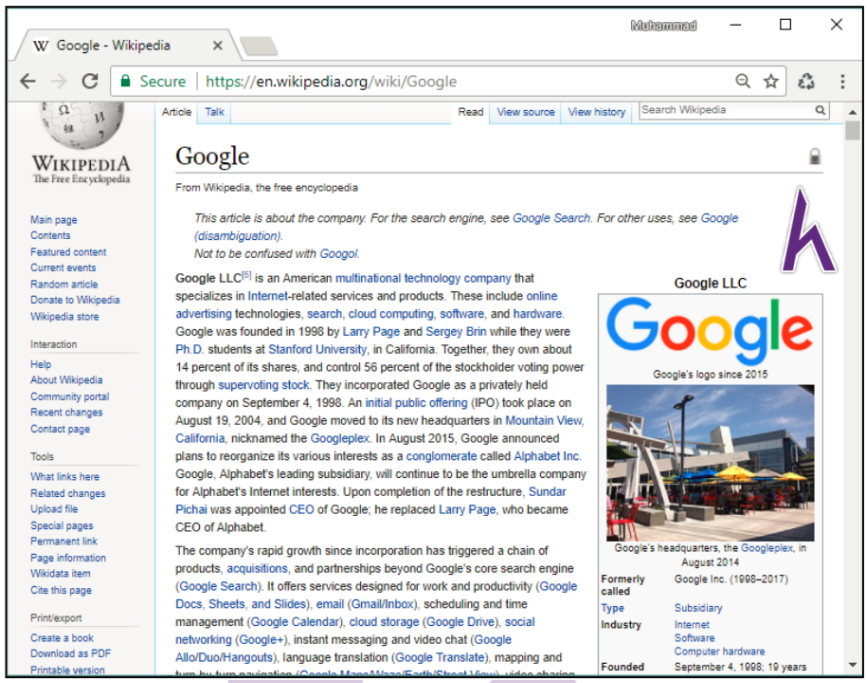
Không phải là một vấn đề lớn để có thể tìm kiếm được thông tin liên quan đến bất kỳ ai như trên mạng internet, truyền thông xã hội, trang web chính thức và các nguồn khác sẽ có nhiều thông tin về người dùng là không chính xác, nhưng một tập hợp thông tin có thể đáp ứng các yêu cầu của kẻ tấn công và kẻ tấn công đó có thể thu thập đủ thông tin bằng khả năng của hắn.

Dưới đây là các kỹ thuật thường được sử dụng bởi tin tặc:

- Thăm dò qua các công cụ tìm kiếm
- Thăm dò qua các kỹ thuật tiến bộ của Google Hacking
- Thăm dò qua các trang web mạng xã hội
- Thăm dò qua các trang mạng
- Thăm dò qua Email
- Thăm dò qua tình báo cạnh tranh
- Thăm dò qua WHOIS
- Thăm dò qua DNS
- Thăm dò qua mạng
- Thăm dò qua kỹ thuật xã hội

Thăm dò thông qua công cụ tìm kiếm

Cách cơ bản nhất rất nhạy và cũng là cách **thăm dò thông qua các công cụ tìm kiếm**. Công cụ tìm kiếm trích xuất thông tin về thực thể bạn đã tìm kiếm từ Internet. Bạn có thể mở trình duyệt web và thông qua bất kỳ công cụ tìm kiếm nào như **Google** hoặc **Bing**, tìm kiếm bất kỳ tổ chức nào. Kết quả thu thập thông tin có sẵn trên Internet.



Ví dụ, tìm kiếm Google sẽ hiển thị thông tin về công cụ tìm kiếm phổ biến nhất thế giới. Thông tin này bao gồm vị trí đặt trụ sở chính, ngày tổ chức thành lập, tên người sáng lập, số lượng nhân viên,tổ chức chính và trang web chính thức của tổ chức. Bạn có thể di chuyển đến các trang web chính thức của nó để có thêm thông tin hoặc bất kỳ trang web nào khác để nhận thông tin về nó.

Ngoài thông tin có sẵn công khai, các trang web và bộ nhớ Cache của công cụ tìm kiếm cũng có thể cung cấp thông tin không có sẵn, được cập nhật hoặc sửa đổi trên trang web chính thức.

Tìm kiếm các tổ chức công khai và các trang web bị hạn chế

Trong quá trình thu thập thông tin, kẻ tấn công cũng thu thập thông tin từ các trang web chính thức của tổ chức bao gồm cả **URLs công khai** và **URLs bị hạn chế**. Các trang web chính thức có thể được tìm thông qua các công cụ tìm kiếm như Google, Bing và các công cụ tìm kiếm khác. Để tìm URLs bị hạn chế của một tổ chức, bằng cách sử dụng phương pháp thử và lỗi, sử dụng các dịch vụ khác nhau để có thể lấy thông tin từ các trang web như www.netcraft.com.

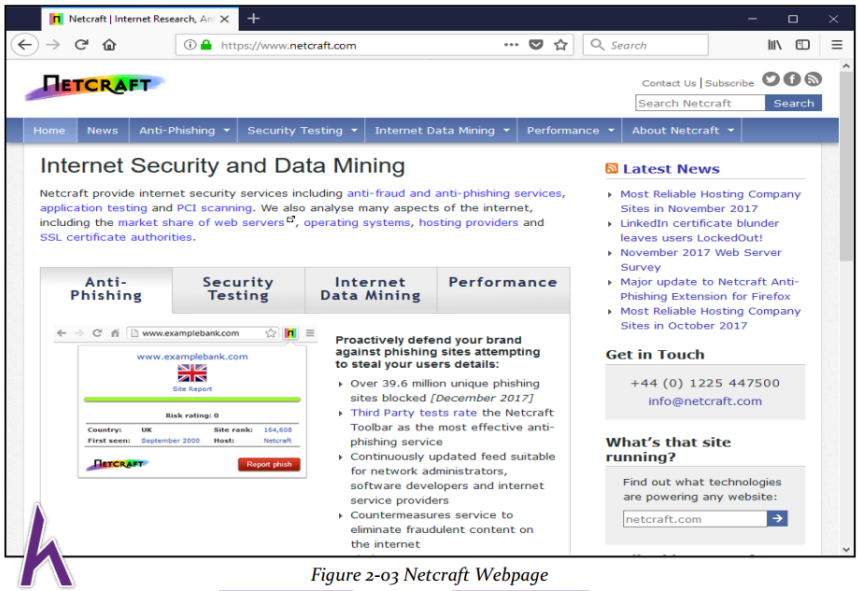


Figure 2-03 Netcraft Webpage

Thu thập thông tin vị trí

Sau khi đã thu thập được các thông tin cơ bản thông qua các công cụ tìm kiếm và các dịch vụ khác nhau giống như Netcarft và Shodan. Bạn có thể thu thập các thông tin cục bộ như vị trí thực của trụ sở với xung quanh, vị trí của văn phòng chi nhánh và thông tin liên quan khác từ vị trí trực tuyến và dịch vụ bản đồ.

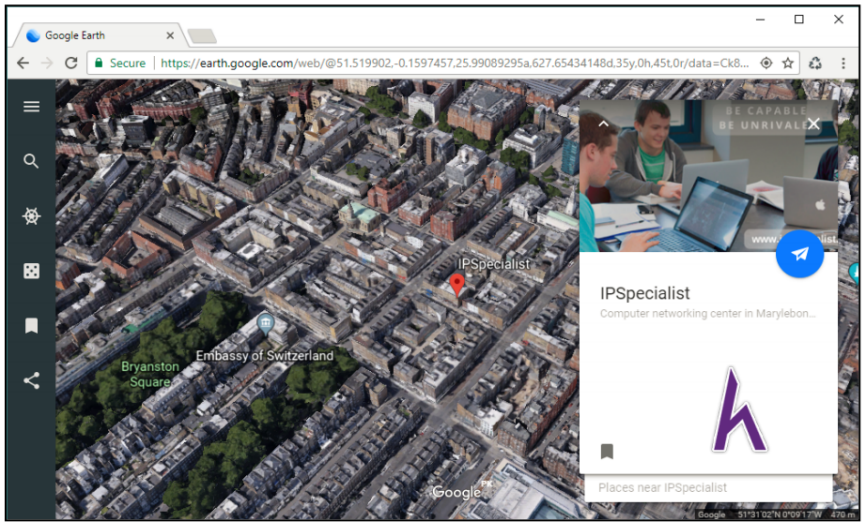


Figure 2-04 Collection of Location Information

Một vài những dịch vụ trực tuyến phổ biến nhất như:

- Ứng dụng bản đồ Google Earth
- Google Map
- Bing Map
- Wikimapia
- Yahoo Map
- Các dịch vụ định vị và bản đồ khác

Dịch vụ tìm kiếm người trực tuyến (People Search Online Services)

Có một số dịch vụ trực tuyến, được sử dụng phổ biến để xác định số điện thoại, địa chỉ hay mọi người.

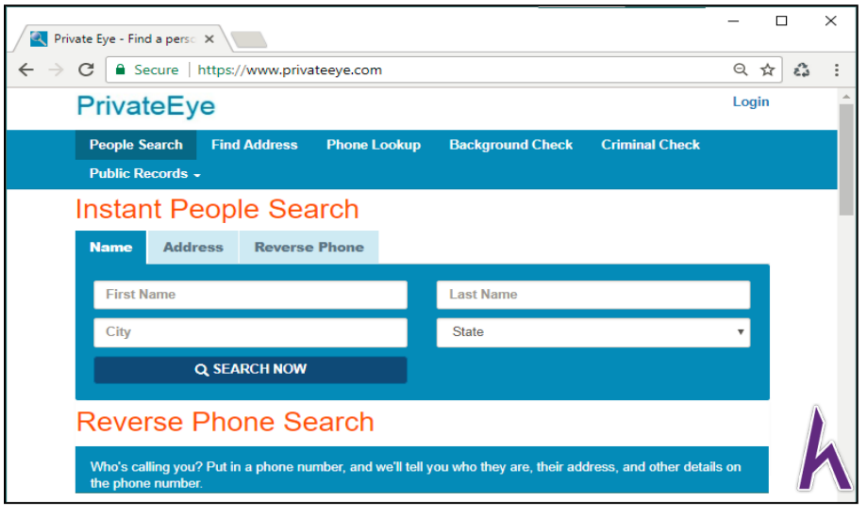


Figure 2-05 Online People Search Service

Một vài trang web bao gồm:

- www.privateeye.com
- www.peoplesearchnow.com
- www.publicbackgroundchecks.com
- www.anywho.com
- www.intelius.com
- www.4111.com
- www.peoplefinders.com

Thu thập thông tin từ các dịch vụ tài chính

Có một số các dịch vụ tài chính được cung cấp bởi các công cụ tìm kiếm khác nhau, chúng cung cấp thông tin tài chính của các tổ chức quốc tế đã được biết đến. Chỉ cần tìm kiếm các tổ chức được nhắm tới là mục tiêu của bạn, bạn có thể nhận được thông tin tài chính từ các tổ chức này. Google và Yahoo là một trong số những dịch vụ tài chính trực tuyến phổ biến nhất:

- www.google.com/finance
- Finance.yahoo.com

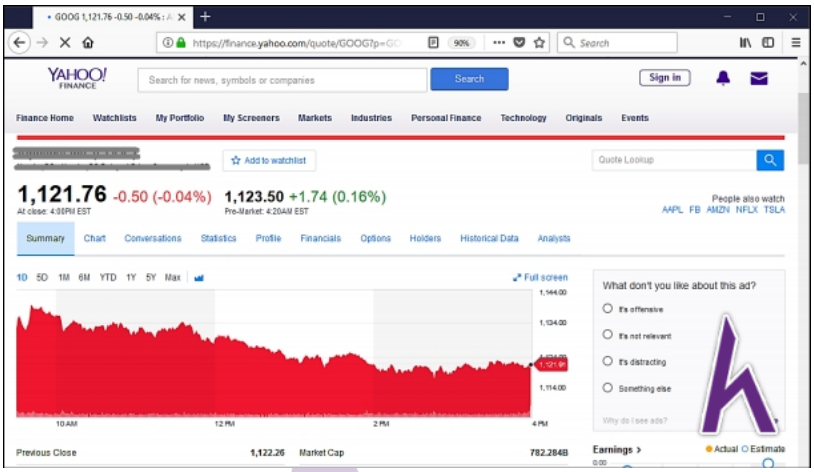

YAHOO! FINANCE
Search for news, symbols or companies
Search
Sign in
Finance Home
Watchlists
My Portfolio
My Screeners
Markets
Industries
Personal Finance
Technology
Originals
Events
Add to watchlist
Quote Lookup
1,121.76 -0.50 (-0.04%)
At close: 4:00PM EST
1,123.50 +1.74 (0.16%)
Pre-Market: 4:20AM EST
People also watch
AAPL FB AMZN NFLX TSLA
Summary
Chart
Conversations
Statistics
Profile
Financials
Options
Holders
Historical Data
Analysts
1D 5D 1M 6M YTD 1Y 5Y Max
Full screen
What don't you like about this ad?
It's offensive
It's not relevant
It's distracting
Something else
Why do I see ads?
Previous Close
1,122.26
Market Cap
782.284B
Earnings
Actual
Estimate

Figure 2-06 Financial Services

Thăm dò dấu vết thông qua trang web công việc

Trong các trang web công việc, công ty cung cấp vị trí tuyển dụng cho mọi người, cung cấp thông tin và danh mục đầu tư của tổ chức của họ cũng như các bài đăng về công việc. Thông tin này bao gồm vị trí công ty, thông tin ngành, thông tin liên lạc, thông tin liên hệ, số lượng nhân viên, yêu cầu công việc, phần cứng và thông tin mềm. Tương tự, trên các trang web việc làm này, bằng một công việc giả mạo, thông tin cá nhân có thể được thu thập từ một cá nhân mà được nhắm làm mục tiêu. Một số trang web công việc phổ biến như:

- www.linkedIn.com
- www.monster.com
- www.indeed.com
- www.careerbuilder.com

Theo dõi mục tiêu bằng cách sử dụng cảnh báo

Google, Yahoo, và những dịch vụ cảnh báo khác cung cấp dịch vụ theo dõi nội dung với tính năng cảnh báo, thông báo đến cho các thuê bao có thông tin mới nhất và cập nhật liên quan đến chủ đề đã đăng ký.

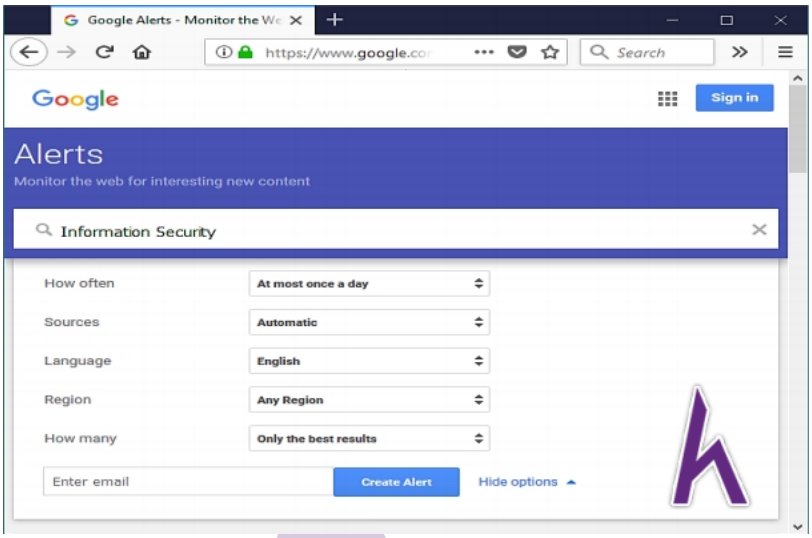


Figure 2-07 Alert Service by Google

Thu thập thông tin bằng cách sử dụng nhóm, diễn đàn và blog

Các nhóm, diễn đàn, blog và cộng đồng có thể là nguồn thông tin nhạy cảm tuyệt vời. Việc tham gia với một ID giả mạo trên các nền tảng này và đến với phòng kín cho nhóm của tổ chức mục tiêu không phải là vấn đề lớn đối với bất kỳ ai. Bất kỳ nhóm chính thức hay không chính thức đều có thể dò rỉ thông tin nhạy cảm.

Lần theo dấu vết bằng cách sử dụng kỹ thuật nâng cao của Google Hacking

Công cụ khai thác tìm kiếm nâng cao của Google

Một vài tùy chọn tiến bộ có thể được sử dụng để tìm kiếm một chủ đề cụ thể bằng cách sử dụng công cụ tìm kiếm. Nhà điều hành tìm kiếm tiến bộ giúp tìm kiếm phù hợp hơn và tập trung vào một chủ đề nhất định. Một số nhà điều hành tìm kiếm bằng google như:

Nhà điều hành tìm kiếm nâng cao	Miêu tả
Trang web	Tìm kiếm kết quả trong miền đã cho
Liên quan	Tìm kiếm các trang web tương tự
Bộ nhớ đệm	Hiển thị các trang web được lưu trữ trên bộ nhớ đệm
Kết nối	Liệt kê các trang web có liên kết đến một trang web cụ thể
Allintext :	Tìm kiếm các trang web chứa từ khóa cụ thể
Intext :	Tìm kiếm các tài liệu chứa từ khóa cụ thể
Allintitle :	Tìm kiếm các trang web có chứa từ khóa cụ thể trong tiêu đề
Intitle :	Tìm kiếm các tài liệu có chứa từ khóa cụ thể trong đầu đề
Allinurl :	Tìm kiếm các trang web có chứa từ khóa cụ thể trong URL
Inurl :	Tìm kiếm các tài liệu có chứa từ khóa cụ thể trong URL

Đối với tìm kiếm nâng cao của Google, bạn cũng có thể truy cập URL sau:

https://www.google.com/advanced_search

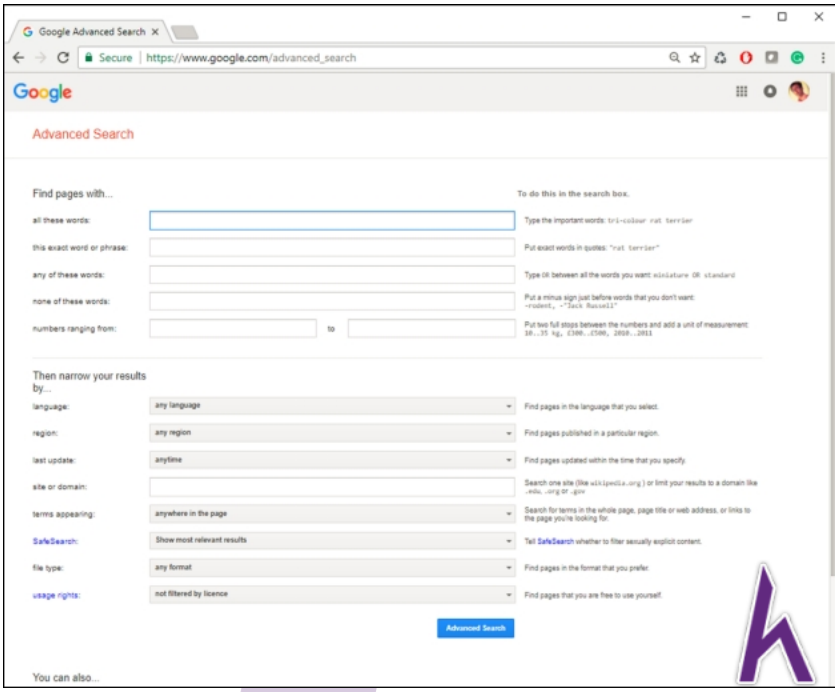


Figure 2-08 Footprinting with Google Advanced Search

Cơ sở dữ liệu Google Hacking (GHDB)

Google hacking, **Google Dorking** là sự kết hợp của các kỹ thuật hacking máy tính để tìm thấy các lỗ hổng bảo mật mạng ca một tổ chức và các hệ thống bằng cách sử dụng tìm kiếm của Google và các ứng dụng khác được cung cấp bởi Google.

Johnny Long là người đã phổ biến rộng rãi Google hacking. Ông đã phân loại các truy vấn trong cơ sở dữ liệu được gọi là cơ sở dữ liệu Google Hacking. Cơ sở dữ liệu đã được phân loại thuộc các truy vấn được thiết kế để khai thác thông tin. Những thông tin này có thể nhạy cảm và không có sẵn một cách công khai. Google Hacking được sử dụng để tăng tốc độ tìm kiếm. Như đã hiện rõ trong hình, thông qua www.exploit-db.com, bạn có thể tìm kiếm GHDB hoặc duyệt qua danh mục GHDB. Tương tự, www.hackersforcharity.org cũng là một nền tảng trực tuyến cho GHDB.

Nhấp vào URL dưới đây:

https://www.exploit-db.com/google-hacking-database/

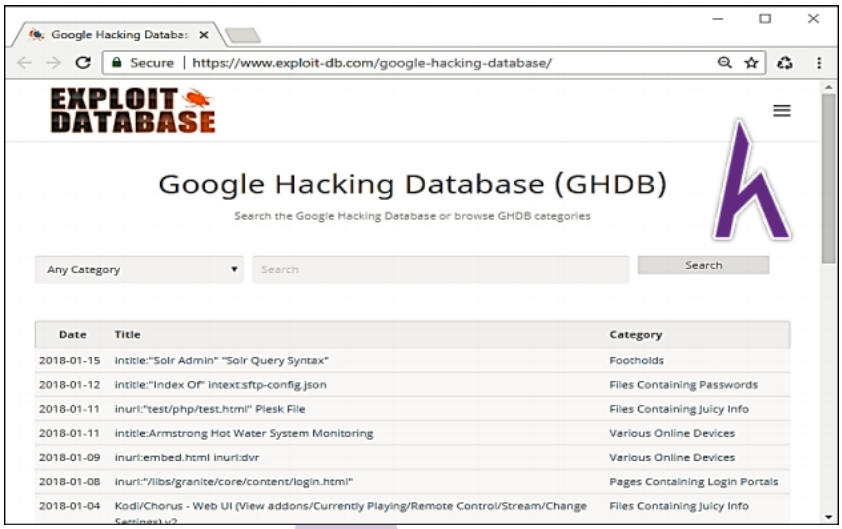


Figure 2-09 Google Hacking Database

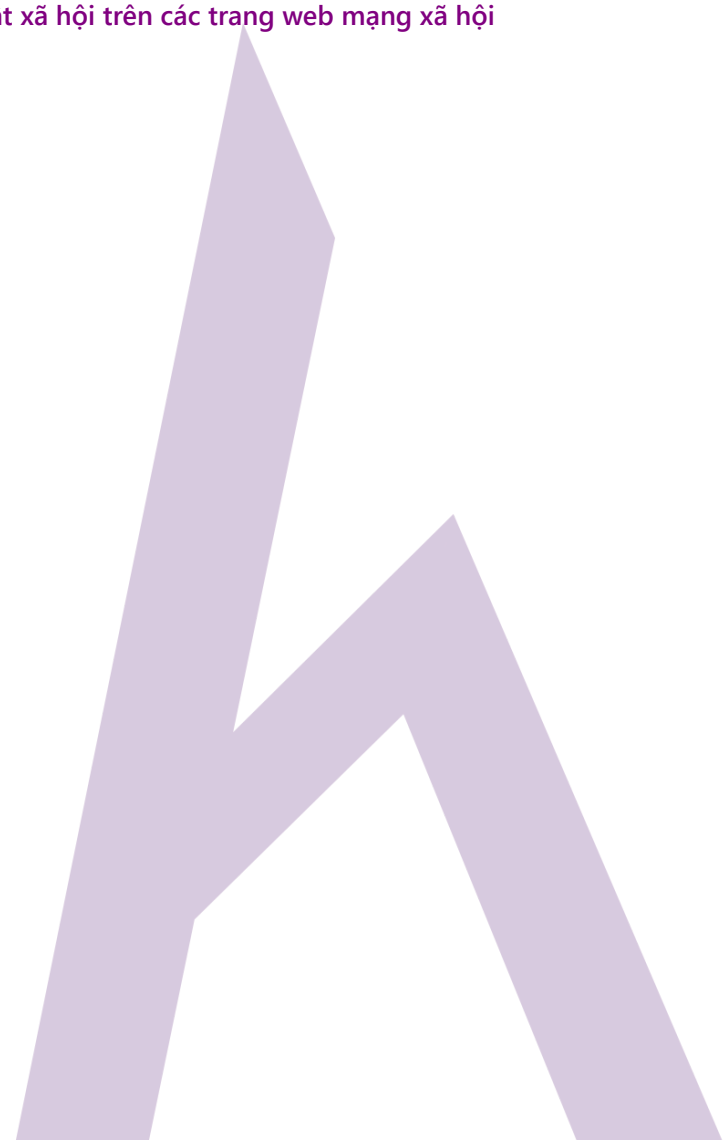
Cơ sở dữ liệu Google Hacking cung cấp các thông tin đã được cập nhật hữu ích cho việc khai thác như vị trí, thư mục nhạy cảm, tệp dễ bị tấn công, thông báo lỗi và nhiều những hữu ích khác nữa.

Thăm dò dấu vết thông qua các trang web mạng xã hội

Kỹ thuật xã hội

Social Engineering trong an ninh thông tin đề cập đến kỹ thuật thao túng & phân tích tâm lí. Thủ thuật này được sử dụng để thu thập thông tn từ các trang mạng xã hội khác nhau và các nền tảng khác từ những người lừa đảo, xâm nhập và lấy thông tin để gần với mục tiêu.

Footprinting sử dụng kỹ thuật xã hội trên các trang web mạng xã hội



Social Networking là một trong những nguồn thông tin tốt nhất trong những nguồn thông tin. Trang mạng xã hội phổ biến và được sử dụng rỗng rãi khác đã khiến cho người khác dễ tìm kiếm ai đó, tìm hiểu về ai đó, bao gồm các thông tin cá nhân cơ bản cũng như một số thông tin nhạy cảm.

Các tính năng nâng cao trên các trang web mạng xã hội này cũng cung cấp các thông tin cập nhật. Một số ví dụ về dấu vết qua các trang mạng xã hội có thể tìm thấy trên Facebook, Twitter, LinkedIn, Instagram và các trang mạng xã hội khác.

Figure 2-10 Social Networking Sites

Social Networking không chỉ là nguồn vui chơi, mà nó còn kết nối con người lại với nhau theo cách cá nhân, chuyên nghiệp và truyền thống. Nền tảng của Social Networking có thể cung cấp thông tin đầy đủ về một cá nhân bằng cách tìm kiếm mục tiêu đó. Tìm kiếm Social Networking làm cho mọi người hay một tổ chức mang lại được rất nhiều thông tin như hình ảnh của mục tiêu, thông tin cá nhân và chi tiết liên hệ, v.v.

Hoạt động của người sử dụng	Thông tin	Những kẻ tấn công chiếm được
Bảo mật tiểu sử	Ảnh	Những thông tin bao gồm các thông tin cá nhân, ảnh, v.v. Kĩ thuật xã hội
	Số điện thoại liên hệ	
	Địa chỉ email	
	Ngày sinh	
	Địa chỉ	
	Chi tiết công việc	
Mọi người cập nhật trạng	Thông tin cá nhân mới nhất	Nền tảng & công nghệ thông tin Vị trí mục tiêu Danh sách nhân viên/ bạn bè/ gia đình. Loại hình kinh doanh
	Vị trí mới nhất	
	Thông tin bạn bè và gia đình	
	Sở thích và các hoạt động	
	Công nghệ thông tin	
	Thông tin các sự kiện sắp diễn ra	

Table 2-02 Social Engineering

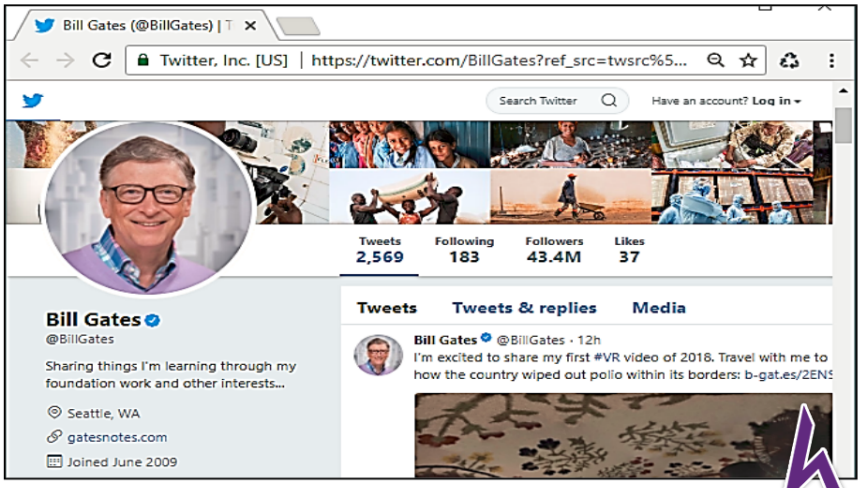
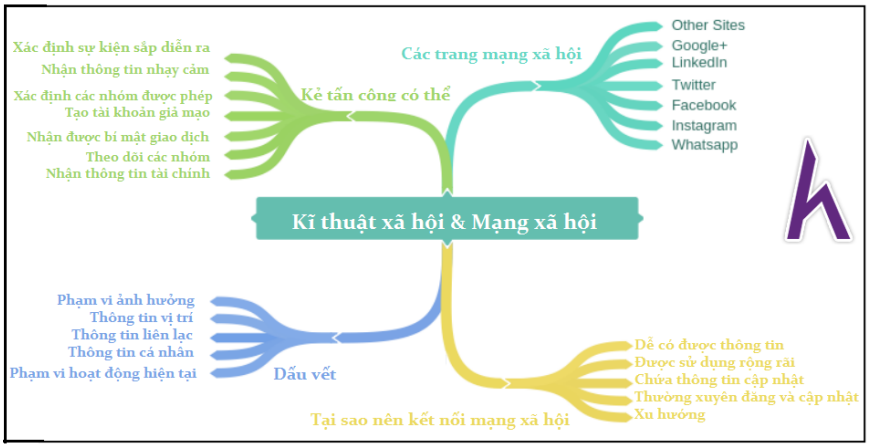


Figure 2-11 Collection of Information from Social Networking

Hình ảnh trong tiểu sử có thể xác định được mục tiêu và có thể thu thập được thông tin cá nhân. Bằng cách sử dụng thông tin cá nhân này, kẻ tấn công có thể tạo tiểu sử giả mạo. Các bài đăng có liên kết với vị trí, hình ảnh và các thông tin vị trí khác để có thể xác định được vị trí của mục tiêu. Lịch trình và các sự kiện cũng có thể tiết lộ các thông tin nhạy cảm. Kẻ tấn công tham gia được vào các vào một số nhóm hay các diễn đàn bằng cách thu thập các thông tin về sở thích hay các hoạt động.

Hơn nữa, các kĩ năng, lịch sử công việc, hay việc làm hiện tại và các thông tin khác. Đây là những thông tin có thể thu thập được một cách dễ dàng và được sử dụng để xác định được loại hình kinh doanh của một tổ chức, công nghệ và các diễn đàn được nhà tổ chức đó sử dụng. Trong các bài đăng, mọi người đăng lên các diễn đàn nhưng họ không nghĩ đến việc những thông tin mà họ đăng lên có thể sẽ chứa đủ thông tin cho kẻ tấn công, hoặc một phần thông tin bắt buộc cho kẻ đó truy cập vào hệ thống của chính họ.

Mind Map



Thăm dò dấu vết trang web (Website Footprinting)

Website Footprinting bao gồm việc giám sát và điều tra về trang web chính thức của tổ chức để đạt được các thông tin như Software đang chạy, phiên bản của acsc phần mềm, hệ điều hành, thư mục Sub, cơ sở dữ liệu, thông tin kịch bản và các chi tiết khác.

Thông tin này có thể thu thập bằng dịch vụ trực tuyến như được định nghĩa trước đó là netcraft.com hoặc bằng cách sử dụng phần mềm như Burp,Suite, Zaproxy, Website Informer, Firebug và các phần mềm khác nữa. Những phần mềm này đem lại những thông tin giống như một loại hình kết nối với các trạng thái và thông tin được sửa đổi lần cuối. Bằng cách nhận được những loại thông tin này, kẻ tấn công có thể kiểm tả mã nguồn,

chi tiết các nhà phát triển, cấu trúc hệ thống tệp và kịch bản lệnh.