Bài: 2.3 Dấu vết & Thăm dò - Cách thăm dò dấu vết (Phần 2)

Xem bài học trên website để ủng hộ Kteam: 2.3 Dấu vết & Thăm dò - Cách thăm dò dấu vết (Phần 2)

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!

Copyright © Howkteam.com

Cách thăm dò dấu vết

Xác định hệ điều hành

Sử dụng các trang web như netcraft.com cũng có thể giúp tìm kiếm các hệ điều hành đang được sử dụng bởi các tổ chức được nhắm làm mục tiêu. Truy cập trang web www.netcraft.com và nhập URL chính thức của tổ chức mục tiêu. Các kết quả trong hình bên dưới được ẩn để tránh các vấn đề về pháp lý.

Copyright © Howkteam.com

Copyright © Howkteam.com

Kết quả mang lại cho tất các trang web liên quan đến miền của tổ chức đó bao gồm các thông tin hệ điều hành và thông tin khác. Nếu bạn nhập một URL hoàn chỉnh, nó sẽ hiển thị chi tiết chuyên sâu của các trang web cụ thể đó.

Copyright © Howkteam.com

Copyright © Howkteam.com

Trang web phổ biến khác tìm kiếm các thông tin chi tiết về các trang web như là Shodan, i.e. www.shodan.io. Công cụ tìm kiếm Shodan cho phép bạn tìm các thiết bị được kết nối như bộ định tuyến, máy chủ, IoT & các thiết bị khác bằng cách sử dụng nhiều bộ lọc khác nhau.

Copyright © Howkteam.com

Truy cập URL dưới đây: www.shodan.io

Copyright © Howkteam.com

Copyright © Howkteam.com

Hiện giờ, việc tìm kiếm của một vài dịch vụ như **CSR1000v** được thể hiện trong hình ảnh trang kế tiếp:

Copyright © Howkteam.com

Copyright © Howkteam.com

Việc tìm kiếm của dịch vụ CSR1000v mang lại 416 kết quả cùng với địa chỉ IP, thông tin phiên bản phần mềm Cisco IOS, thông tin vị trí và những chi tiết khác.

Dấu vết trang web bằng cách sử dụng Web Spiders

Web Spiders hay **Web Crawlers** là những bots mạng được sử dụng để thực hiện duyệt web tự động có hệ thống trên **World Wide Web**. Duyệt web này được nhắm mục tiêu đến một trang web để thu thập thông tin cụ thể như tên, địa chỉ email.

Copyright © Howkteam.com

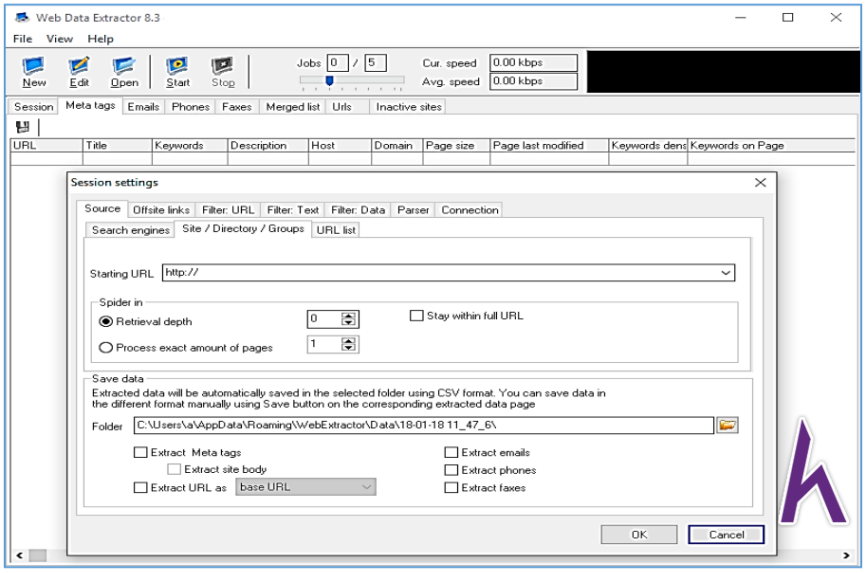

Figure 2-16 Web Data Extractor Application (Web Spider)

Theo dõi toàn bộ trang web

Copyright © Howkteam.com

Mirroring a website là quá trình **phản chiếu toàn bộ** trang web trong hệ thống cục bộ. Việc tải toàn bộ trang web lên hệ thống cho phép kẻ tấn công sử dụng, kiểm tra trang web, thư mục, cấu trúc và tìm ra được các lỗ hổng khác từ bản sao trang web khi được tải xuống.

Việc sao chép này xảy ra trong môi trường ngoại tuyến. Thay vì gửi nhiều bản sao tới máy chủ web, đây là cách để tìm ra các lỗ hổng trên trang web.

Các công cụ Mirroring sẵn có thể tải xuống một trang web. Ngoài ra, chúng có khả năng xây dựng tất xả các thư mục, THTML và các tệp khác từ máy chủ đến một thư mục cục bộ.

Copyright © Howkteam.com

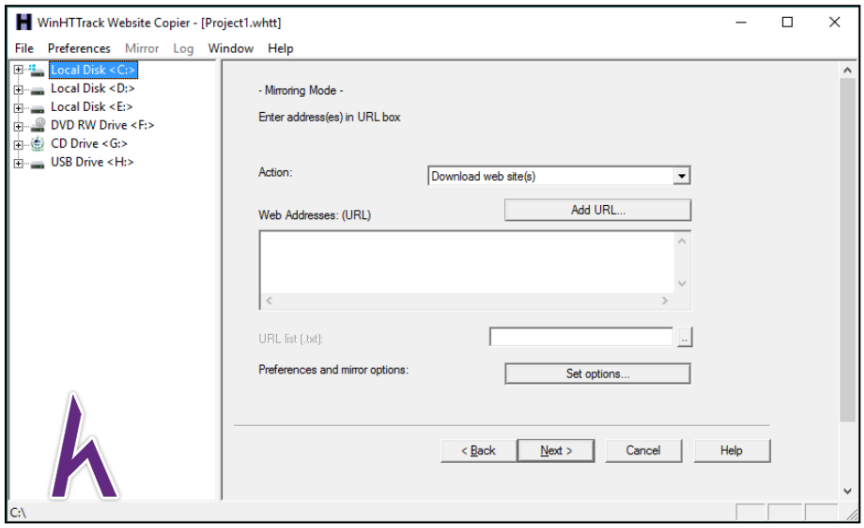

Figure 2-17 WinHTTrack Website Copier

Copyright © Howkteam.com

Công cụ theo dõi các trang web (Website Mirroring Tools)

Công cụ **Website mirroring** bao gồm các phần mềm cung cấp **Web mirroring**. Một vài những công cụ đó như:

Software	Websites
Win HTTrack Website Copier	https://www.httrack.com/page/2/
Surf offline Professional	http://www.surfoffline.com/
Black Widow	http://softbytelabs.com
NCollector Studio	http://www.calluna-software.com
Website Ripper Copier	http://www.tensons.com
Teleport Pro	http://www.tenmax.com
Portable Offline Browser	http://www.metaproducts.com
PageNest	http://www.pagenest.com
Backstreet Browser	http://www.spadixbd.com
Offline Explorer Enterprise	http://www.metaproducts.com
GNU Wget	http://www.gnu.org.com
Hooeey Webprint	http://www.hooeeywebprint.com

Copyright © Howkteam.com

Trích dẫn thông tin các trang web (Extract Website Information)

Archive.com là một dịch vụ trực tuyến cung cấp phiên bản lưu trữ của các trang web. Kết quả bao gồm một bản tóm tắt của trang web đó: Tóm tắt về Mine-type Count, tóm tắt TLD/HOST/Domain, một sơ đồ trang web và ngày tháng, chế độ xem lịch và các thông tin khác.

Trích thông tin bằng cách sử dụng công cụ Wayback

1. Truy cập vào URL dưới đây:

> http://web.archive.org

2. Tìm trang web
3. Chọn năm từ lịch biểu.

Copyright © Howkteam.com

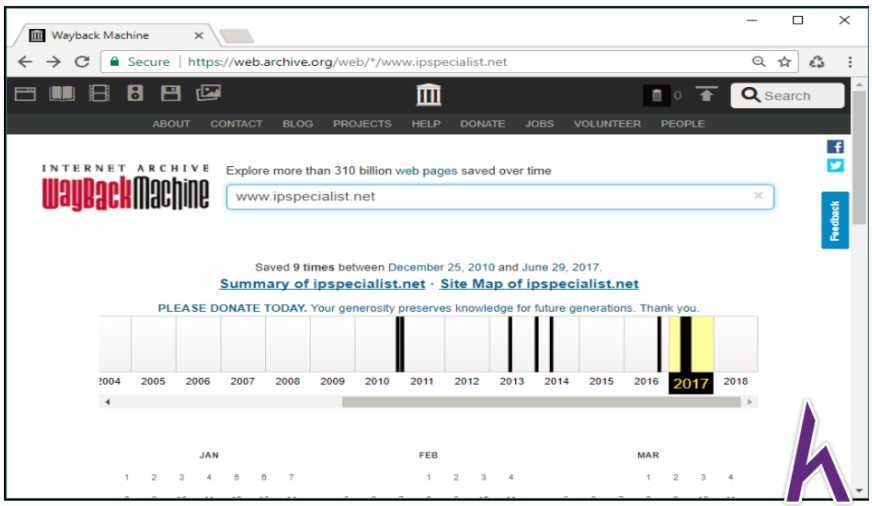

Figure 2-19 Archive.com Wayback Machine

Copyright © Howkteam.com

4. Chọn ngày từ những ngày được tô sáng.

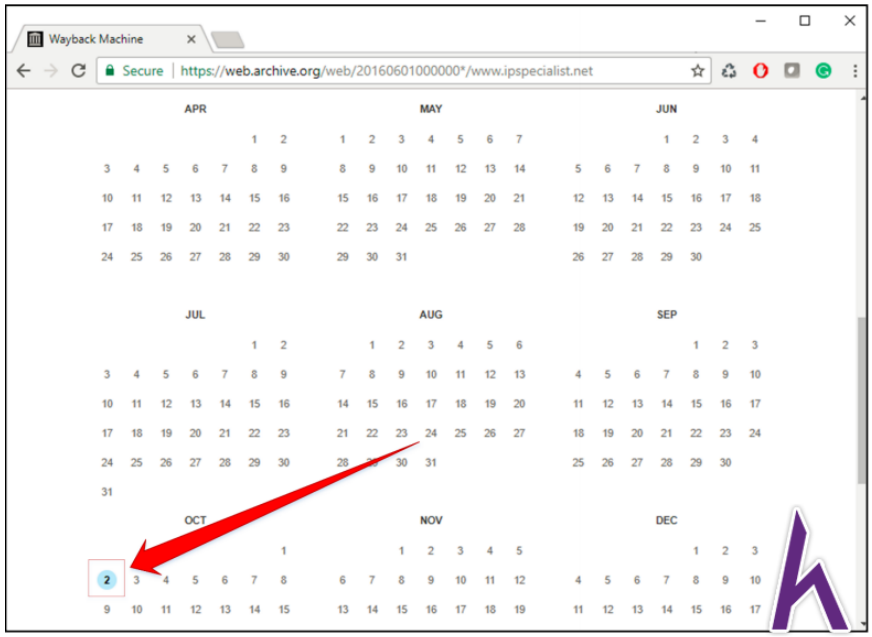

Figure 2-20 Select Date

5. Sau đây là ảnh chụp nhanh của trang web vào ngày 2 tháng 10 năm 2016

Copyright © Howkteam.com

Theo dõi cập nhật các trang web (Monitoring Web Updates)

Website-Watcher và những công cụ có sẵn khác đều cung cấp việc giám sát các trang web. Những công cụ này tự động kiểm tra những thay đổi và cập nhật khi được thực hiện cho các trang web mục tiêu.

Copyright © Howkteam.com

Copyright © Howkteam.com

Công cụ Monitoring	Websites
Change Detection	http://www.changedetection.com
Follow That Page	http://www.followthatpage.com
Page2RSS	http://page2rss.com
Watch That Page	http://www.watchthatpage.com
Check4Change	https://addons.mozilla.org
OnWebChange	http://onwebchange.com
Infominder	http://www.infominder.com
TrackedContent	http://trackedcontent.com
Websnitcher	https://websnitcher.com
Update Scanner	https://addons.mozilla.org

Copyright © Howkteam.com

Dấu vết Email (Email Footprinting)

Email có **vai trò quan trọng** trong việc điều hành doanh nghiệp tổ chức. Email còn là một trong những cách chuyên nghiệp được sử dụng rộng rãi, phổ biến nhất trong giao tiếp bởi mọi tổ chức. Việc giao tiếp với đối tác, nhân viên, đối thủ, nhà thầu và những người khác được đòi hỏi trong việc điều hành một tổ chức. Nội dung của email rất quan trọng, nó thực sự có giá trị đối với kẻ tấn công.

Copyright © Howkteam.com

Nội dung có thể bao gồm thông tin về phần cứng và phần mềm, thông tin người dùng, thông tin mạng và thiết bị bảo mật, thông tin tài chính. Tất cả những thông tin đó là rất giá trị đối với việc thâm nhập và kẻ tấn công.

Polite Mail là công cụ hữu ích cho **Email footpriting**. **Polite Mail** theo dõi giao tiếp bằng email với Microsoft Outlook. Sử dụng công cụ này, với một danh sách các địa chỉ email của tổ chức mục tiêu, các link (liên kết) độc có thể được gửi và theo dõi các sự kiện cá nhân.

Truy tìm email bằng tiêu đề email có thể tiết lộ thông tin sau:

Copyright © Howkteam.com

- Địa chỉ nơi đến
- Địa chỉ IP người gửi
- Máy chủ Mail của người gửi
- Thông tin thời gian
- Thông tin hệ thống được thẩm định của máy chủ mail người gửi

Tracking Email from Email Header (Theo dõi Email từ Tiêu đề Email)

Theo dõi Email từ thư mời cung cấp tiêu đề của một email cùng với địa chỉ IP, Hop Name và vị trí. Một số ứng dụng trực tuyến và phần mềm cung cấp việc truy cập tiêu đề Email, Email Tracker Pro là một trong những công cụ phổ biến.

Copyright © Howkteam.com

Công cụ theo dõi Email (Email Tracking Tools)

Copyright © Howkteam.com

Công cụ theo dõi Email phổ biến như:

- Email Tracker Pro
- Email Lookup
- Yesware
- Who Read Me
- Contact Monkey
- Read Notify
- Did They Read It
- Get Notify
- Point of Mail
- Trace Email
- G-Lock Analytics

Cạnh tranh thông minh (Competitive Intelligence)

Thu thập **cạnh tranh thông minh** là một cách thu thập thông tin, phân tích và thu thập thống kê các đối thủ cạnh tranh. Quá trình đó không có sự can thiệp vì nó là quá trình thu thập thông tin thông qua các nguồn khác nhau. Một vài nguồn cơ bản của việc cạnh tranh thông minh như:

Copyright © Howkteam.com

- Trang web chính thức (Offcial Websites)

Copyright © Howkteam.com

- Quảng cáo công việc (Job Advertisements)
- Thông cáo báo chí (Press releases)
- Báo cáo thường niên (Annual Reprts)
- Danh mục sản phẩm (Product Catalogs)
- Báo cáo quy định (Regulatory Reports)
- Đối tác, nhà phân phối & Người cung cấp (Agents, distributors & Supplier)

Copyright © Howkteam.com

Thu thập cạnh tranh thông minh (Competitive Intelligence Gathering)

Copyright © Howkteam.com

Để có được những thông tin cạnh tranh, bạn nên tìm hiểu các trang web như **EDGAR**, **LexisNexis**, **Business Wire & CNBC**. Những trang web này thu thập thông tin và những bản báo cáo của các công ty bao gồm tin tức hợp pháp, thông cáo báo chí, thông tin tài chính, báo cáo phân tích, và những dự án sắp tới và kế hoạch dự định. Để biết thêm nhiều thông tin, hãy tìm hiểu những trang web sau:

Websites	URL
EDGAR	https://www.sec.gov/edgar.shtml
LexisNexis	https://risk.lexisnexis.com
Business Wire	www.businesswire.com/portal/site/home/
CNBC	www.cnbc.com
Hoovers	www.hoovers.com

Table 2-05 Competitive Intelligence Sources

Thu thập thông tin từ những nguồn này, việc thâm nhập và kẻ tấn công có thể xác định được:

- Công ty bắt đầu từ khi nào?
- Sự phát triển của công ty
- Thẩm quyền của công ty
- Cơ sở của tổ chức
- Kế hoạch và chiến lược
- Thông tin tài chính
- Những thông tin khác

Theo dõi lưu lượng truy cập trang web của công ty được nhắm tới

Những công cụ theo dõi trang web, đều được sử dụng rộng rãi bởi các nhà phát triển, kẻ tấn công và sự thâm nhập để kiểm tra thông tin trang web. Các công cụ này bao gồm **Web-stat & Alexa** và các công cụ khác chỉ ra thông tin của các vị trí trang web được nhắm tới, tầm nhìn địa lí tới người sử dụng từ khắp thế giới, số lượng người sử dụng trên khắp mọi nơi, người sử dụng từ các quốc gia khác nhau, các trang được xem hàng ngày, thời gian hàng ngày trên các trang web, toàn bộ số lượng các trang web được kết nối, và nhiều thứ khác.

Copyright © Howkteam.com

Công cụ theo dõi lượng truy cập trang web (Website Traffic Monitoring Tools)

Copyright © Howkteam.com

Công cụ	URL
Monitis	http://www.monitis.com/
Web-stat	https://www.web-stat.com/
Alexa	https://www.alexa.com/

Table 2-06 Website Traffic Monitoring Tools

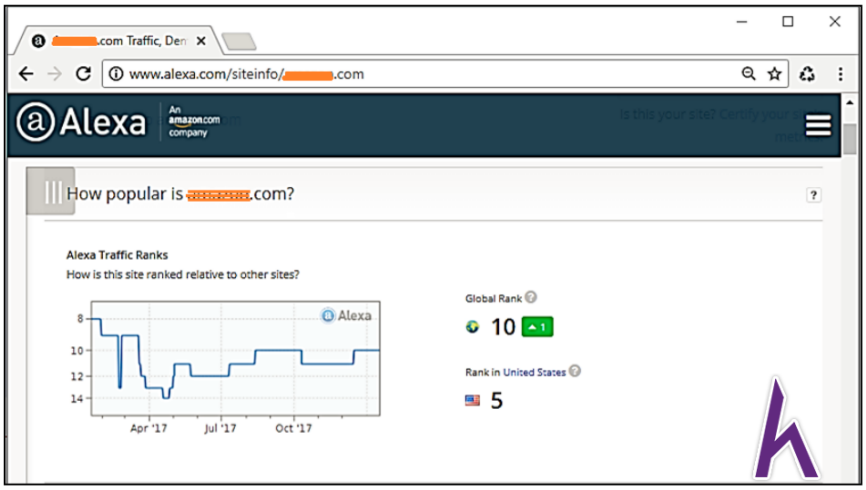

Figure 2-24 Website Statistics using Alexa

Như hình bên trên, trang web phổ biến nhất, Amazon.com đang được tìm kiếm bởi Alexa. Kết quả cho thấy **Alexa Traffic Ranking**, **Global Rank of Website**, **Rank in the United States**. Cuộn xuống trang có hiển thị các kết quả khác nhau như tầm nhìn địa lý của đối tượng, tỷ lệ phần trăm và xếp hạng ở mọi quốc gia và nhiều hơn nữa:

Copyright © Howkteam.com

Tương tự, công cụ khác giống như Web-stat và Monitis theo dõi trang lưu lượng truy cập trang web có thể thu thập tỉ lệ tăng vụt, bản đồ khách truy cập trực tiếp và các thông tin khác.

Copyright © Howkteam.com

Copyright © Howkteam.com

Theo dõi danh tiếng trực tuyến của mục tiêu (Tracking Online Reputation of the Target)

Copyright © Howkteam.com

Danh tiếng của một tổ chức có thể bị theo dõi thông qua các dịch vụ trực tuyến. Online Reputation Management (ORM) cung cấp để theo dõi danh tiếng của tổ chức. Những công cụ này được sử dụng để theo dõi danh tiếng, xếp hạng, thiết lập khai báo khi một tổ chức được biết đến thông qua mạng và nhiều thứ khác.

Công cụ để theo dõi danh tiếng trực tuyến (Tools for Tracking Online Reputation)

Copyright © Howkteam.com

Công cụ	URL
Google Alerts	https://www.google.com
WhosTalkin	http://www.whostalkin.com
Rankur	http://rankur.com
PR Software	http://www.cision.com
Social Mention	http://www.socialmention.com
Reputation Defender	https://www.reputation.com

Copyright © Howkteam.com

Một trong những công cụ theo dõi phổ biến là **Trakur** (www.trackur.com). Bạn có thể tìm kiếm những từ khóa như chỉ dẫn trong hình đã thể hiện kết quả cho Microsoft. Biểu tượng chia ra các kết quả từ những nguồn khác nhau, bạn có thể xem xét kết quả bằng cách lựa chọn mục nhập.

Copyright © Howkteam.com