



MODULE 2

MÔN : AN NINH MẠNG
GVHD: LÊ TỰ THANH

Nhóm 2:

1. Trần Ngọc Tuấn
2. Nguyễn Thế Phương



FOOTPRINTING



IN DẤU CHÂN VÀ GIÁM SÁT

CHƯƠNG 2

Engineered by Hackers. Presented by Professionals.



FOOTPRINTING



BẢO MẬT TIN TỨC



21st May 2010, Chicago, Illinois

Battle Against Data Theft

Một nhận thức sai lầm chung mà tội phạm mạng thường chọn đó là người sử dụng có giá trị cao và đa số người dùng internet đánh giá thấp các nguy cơ truy cập trái phép dữ liệu của họ.

Trong một cuộc khảo sát gần đây được tiến hành bởi avira, 10% người sử dụng Internet đã xác nhận họ đã là nạn nhân của một số hình thức trộm cắp dữ liệu, trong đó có 4% thực tế đã bị tổn thất tài chính và 6% đã là nạn nhân của hành vi trộm cắp danh tính.

Nhưng tội phạm mạng trở nên khéo léo hơn, phát hiện hành vi bắt thường hoặc giảm hiệu suất hệ thống là có thể bảo vệ an ninh rộng hơn.

Sự tinh vi của các ứng dụng là tiềm ẩn nguy cơ không mong muốn (PUAs) có nghĩa là sự hiện diện của họ vẫn không bị phát hiện dài hạn và trả tiền thường xuyên hơn để người dùng tin.

Danh cắp dữ liệu từ e-mail và tài khoản trực tuyến (facebook và ebay) hoặc những phản hồi bắt cần để lừa đảo trực tuyến.

<http://www.itweb.co.za>

FOOTPRINTING



MỤC TIÊU

- Footprinting là gì?
- Mục tiêu của footprinting
- Mối đe dọa của footprinting
- Footprinting mạng Internet
- Cảnh tranh thông minh
- WHOIS footprinting
- DNS footprinting



- Footprinting trên mạng
- Website
- E-mail
- Tấn công google
- Công cụ footprinting
- Biện pháp đối phó footprinting
- Bút thử nghiệm footprinting



FOOTPRINTING



Module Flow



Footprinting
khái niệm



Footprinting
mối đe dọa



Footprinting
phương pháp



Footprinting
công cụ



Footprinting
biện pháp đối phó



Footprinting
bút thử nghiệm

FOOTPRINTING



THUẬT NGỮ FOOTPRINTING

Mã nguồn mở hoặc thu thập thông tin thụ động

thu thập thông tin về mục tiêu từ các nguồn truy cập công cộng

Thu thập thông tin hoạt động

thu thập thông tin thông qua kỹ thuật thăm trên trang web, các cuộc phỏng vấn, và bảng câu hỏi

Footprinting tàng hình

thu thập thông tin từ các nguồn tác giả mà khi đó thông tin không thể được xác định hoặc truy tìm

Footprinting giả

thu thập thông tin có thể được xuất hiện dưới một tên khác nhau trong một nỗ lực để bảo vệ sự riêng tư

Footprinting một tổ chức hoặc cá nhân

thu thập thông tin từ một tổ chức như lịch dựa trên web và máy chủ thư điện tử

Footprinting trên Internet

thu thập thông tin về 1 mục tiêu trên internet

FOOTPRINTING

Footprinting là gì?

Footprinting tham khảo để phát hiện và thu thập càng nhiều thông tin càng tốt về một mục tiêu mạng.



FOOTPRINTING



Objectives of Footprinting



Thu thập thông tin mạng

- Tên domain
- Tên domain nội bộ
- Khối kết nối mạng
- Địa chỉ IP của thẻ truy cập hệ thống
- Giả mạo web/ cá nhân web
- Máy chủ chạy TCP và UDP



Thu thập thông tin hệ thống

- Người dùng và tên nhóm
- Hệ thống biểu ngữ
- Bang định tuyến
- Thông tin SNMP



Thu thập thông tin về tổ chức

- Thông tin nhân viên
- Tổ chức web
- Danh sách công ty

- Giao thức mạng
- Quan điểm VPN
- ACLs
- chạy IDSes
- tín hiệu tương tự/ tín hiệu số điện thoại
- xác thực các cơ chế

- Mô hình hệ thống
- Kiểu hệ thống từ xa
- Tên hệ thống
- Mật khẩu

- Địa chỉ và số điện thoại
- Nền tảng về tổ chức
- Tin tức về các bài viết/ phát hành các bài báo

FOOTPRINTING

Module Flow



Footprinting
Concepts



Footprinting
Threats



Footprinting
Methodology



Footprinting
Tools



Footprinting
Countermeasures



Footprinting
Pen Testing



FOOTPRINTING



Mối đe dọa của Footprinting

Kẻ tấn công thu thập thông tin hệ thống có giá trị như chi tiết tài khoản, hệ thống điều hành và các phiên bản phần mềm khác, tên máy chủ và các chi tiết sơ đồ cơ sở dữ liệu từ kỹ thuật Footprinting.



FOOTPRINTING



Module Flow



Footprinting
Concepts



Footprinting
Threats



Footprinting
Methodology



Footprinting
Tools



Footprinting
Countermeasures



Footprinting
Pen Testing

FOOTPRINTING

Phương thức Footprinting



FOOTPRINTING

Tìm kiếm một công ty thông qua URL



Tìm kiếm các công ty mục tiêu với một số công cụ tìm kiếm như Google hoặc Bing



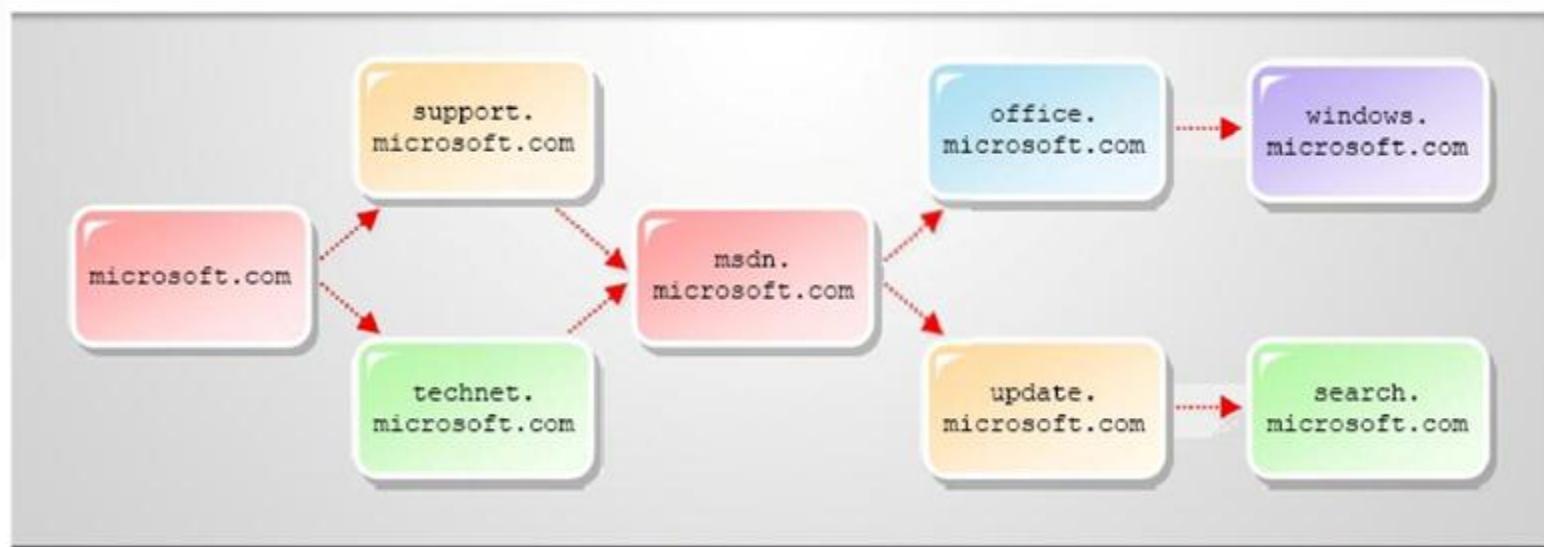
The screenshot shows a Google search results page for the query "microsoft". The search bar at the top contains "microsoft". Below the search bar, it says "About 399,000,000 results (0.12 seconds)". On the left, there's a sidebar with search filters: "Everything", "News", "Blogs", "More", "The web", "Pages from India", "Any time", "Latest", "Past 4 days", "Standard view", "Timeline", and "More search tools". The main search results list includes:

- Microsoft Corporation**
Main site for product information, support, and news.
www.microsoft.com/ - Cached - Similar
Download Center 5 ways to speed up your PC
7 Home Microsoft Windows: Windows 7 ...
Downloads Internet Explorer 8
XP Office
- Microsoft Download Center**
Search All Download CenterSearch Microsoft.com ... Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats ...
www.microsoft.com/downloads/en/default.aspx - Cached - Similar
- Microsoft - Wikipedia, the free encyclopedia**
Microsoft Corporation (NASDAQ: MSFT, HKEX: 4338) is a public multinational corporation based in Redmond, Washington, USA that develops, manufactures, ...
en.wikipedia.org/wiki/Microsoft - 11 hours ago - Cached - Similar

FOOTPRINTING

Xác định vị trí nội bộ URLs

- URL cung cấp một cái nhìn sâu sắc vào các phòng ban khác nhau và các đơn vị kinh doanh trong một tổ chức
- Bạn có thể tìm thấy một công ty nội bộ URL bằng cách dùng thử và phương pháp báo lỗi
- Công cụ tìm kiếm URL nội bộ
 - <http://news.netcraft.com>
 - <http://www.webmaster-a.com/link-extractor-internal.php>



FOOTPRINTING

Trang web công cộng và hạn chế

xác định một công ty có các trang web tư nhân và công cộng

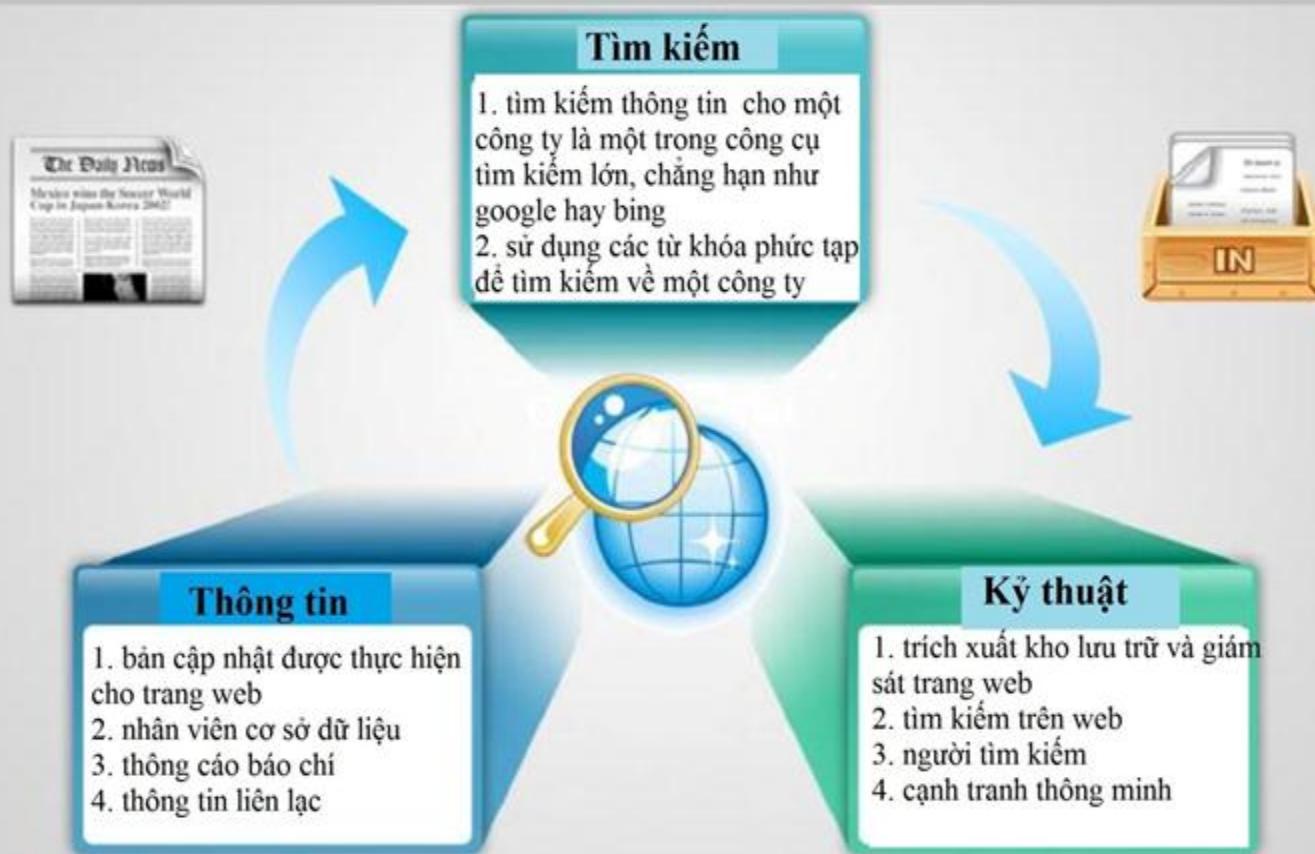


Public website
<http://www.apple.com>

Restricted website
<http://developer.apple.com>

FOOTPRINTING

Tìm kiếm thông tin cho một công ty



FOOTPRINTING



Công cụ để thu thập dữ liệu của công ty

I

Web Data Extractor (<http://www.webextractor.com>)

- trang web dữ liệu trích xuất dữ liệu liên lạc của các công ty mục tiêu (email, điện thoại, fax) từ mạng internet

II

SpiderFoot (<http://www.binarypool.com>)

- spiderfoot có một công cụ footprinting miền mà sẽ lấy hết các trang web trên tên miền đó, cũng như tìm kiếm google, Netcraft, whois, và DNS để thu thập các thông tin công ty

III

Robtex (<http://www.robtex.com>)

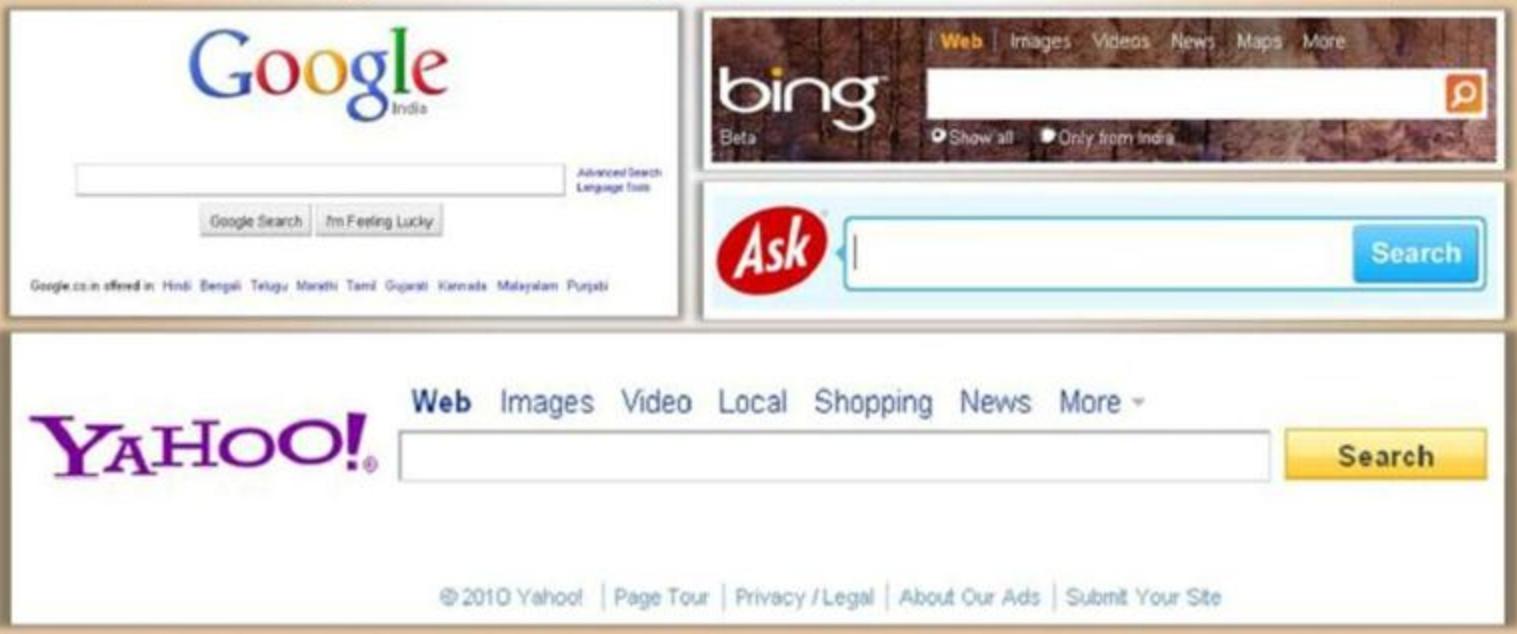
- robtex hệ thống thu thập dữ liệu internet bằng cách sử dụng “robtexbot” tác nhân người dùng là chủ yếu để có được thông tin tiêu đề và meta

FOOTPRINTING



Footprinting thông qua công cụ tìm kiếm

- Kẻ tấn công sử dụng công cụ tìm kiếm để thu thập thông tin về một mục tiêu chủng hạn như nền tảng công nghệ, chi tiết nhân viên, các trang đăng nhập, mạng nội bộ công thông tin, giúp thực hiện kỹ thuật và các kế hoạch khác của các cuộc tấn công hệ thống tiên tiến.
- Bộ nhớ cache của công cụ tìm kiếm có thể cung cấp các thông tin nhạy cảm đã được gỡ bỏ từ các trang web trên toàn thế giới (WWW).



The image displays four search engine interfaces side-by-side:

- Google India:** Shows the classic Google logo with "India" at the bottom. It includes a search bar, "Advanced Search" and "Language Tools" links, and buttons for "Google Search" and "I'm Feeling Lucky". Below the search bar, it says "Google.co.in offered in: Hindi Bengali Telugu Malayalam Tamil Gujarati Kannada Malayalam Punjabi".
- Bing Beta:** Shows the Bing logo with "Beta" below it. It has a search bar with options "Show all" and "Only from India", and links for "Web", "Images", "Videos", "News", "Maps", and "More".
- Ask:** Shows the Ask logo with a red circle. It has a search bar and a "Search" button.
- Yahoo!**: Shows the Yahoo! logo in purple. It has a search bar and links for "Web", "Images", "Video", "Local", "Shopping", "News", and "More".

At the bottom of the image, there is footer text: "© 2010 Yahoo! | Page Tour | Privacy / Legal | About Our Ads | Submit Your Site".

FOOTPRINTING



Thu thập vị trí thông tin



- Sử dụng công cụ GoogleEarth để có được vị trí của mọi nơi



FOOTPRINTING



Hình ảnh vệ tinh của một nơi cư trú



FOOTPRINTING



Người tìm kiếm

Người tìm kiếm trả về các thông tin sau đây về một người

địa chỉ ở

số hợp đồng

ngày tháng năm sinh

địa chỉ e-mail

vết tinh hình ảnh của nhà ở tư nhân



Bạn có thể tìm thấy thông tin cá nhân người sử dụng qua dịch vụ tìm kiếm trực tuyến

Premium Public Records (24)

All INTELUS US SEARCH PeopleSmart

 Bill U Clinton (age: 76)
94044 PACIFICA, CA - [view details](#)

 Bill J Clinton (age: 66)
61571 WASHINGTON, IL - [view details](#)

 B.R Clinton (age: 82)
San Mateo, CA - [view details](#) | background check

 100 entries for Bill Clinton found in:
California, Florida, Texas, New Jersey, Tennessee, New York,
Missouri, Arizona, Georgia, Oklahoma, ...

Your Report:

Overview >

People Search

Report

Death Records

Marriage And
Divorce Records

[View All](#)

Your Search:

Name: Lori Ortiz
15050 NE 99th Way
Bellevue, WA 98004

Address: 15050 NE 99th Way
Bellevue, WA 98004

Phone Number: (425) 555-1000
Aliases: 1) Lorry Ortiz
2) Samatha Ortiz

Age: 37

FOOTPRINTING

Mọi người tìm kiếm bằng cách sử dụng <http://pipl.com>



Pipl sử dụng một kỹ thuật được gọi là trang web sâu để trích xuất thông tin về người

Web sâu đề cập đến một kho lưu trữ rộng lớn của nội dung cơ bản, chẳng hạn như tài liệu trong cơ sở dữ liệu trực tuyến mà trình thu thập dữ liệu web có mục đích chung không thể đạt được



The most comprehensive people search on the web

Name Email Username Phone Business

First Name Last Name City State Country

[What's so different about pipl?](#)

[Terms](#) [Privacy](#) [Directory](#) [Contact](#)
©2006-2010 Pipl

FOOTPRINTING

Mọi người tìm kiếm máy chủ trực tuyến

People Search

Name Address Email Social Security # Social Net Search

First Name MI Last Name

State All States Advanced Search

[View Sample Report](#)

What is a People Search?

People Search is great way to find and reconnect with family, old friends, relatives — just about anyone! People Search reports include phone numbers, address history, ages, birthdays, household members, home value, income and more.

<http://www.intelius.com>

BestPeopleSearch.com

How can we help with your people search today? Select from Free People Search, Instant People Search, or Professional People Searches.

Free  **Instant**  **Professional** 

Free & Instant People Search

Do It Yourself Instant People Search

Free & Instant Private Investigator

Find and help Law-Offices, Collection agencies, Detainees, Private Investigators, and other professionals! Visit Best People Search. As a trusted name since 1998, we believe in **honesty, integrity, and quality service**.

<http://www.bestpeoplesearch.com>

People-Search-America.com

PEOPLE SEARCH
Put information on any phone, mobile cell phone, business phone, fax phone and even internet numbers. Research names, addresses, email and more. Find names, addresses, email and more.

* Name: * State:

REVERSE PHONE LOOKUP
Find information on any phone, mobile cell phone, business phone, fax phone and even internet numbers. Research names, addresses, email and more. Find names, addresses, email and more.

SOCIAL SECURITY
Investigate and research into social security numbers. Find information on any phone, mobile cell phone, business phone, fax phone and even internet numbers. Research names, addresses, email and more.

<http://people-search-america.com>

AnyWho

stop hunting. start finding.

FINDING PEOPLE, PLACES, AND BUSINESSES

FIND A BUSINESS

FIND A PERSON

GET OUR FREE app for the iPhone's YELPWHO

FIND **LOCATION:** **Q FIND**

YELPING.COM

<http://www.anywho.com>



FOOTPRINTING



Mọi người tìm kiếm các dịch vụ trực tuyến



Yahoo People Search

<http://people.yahoo.com>



123 People Search

<http://www.123people.com>



Wink People Search

<http://wink.com>



People Finders

<http://www.peoplefinders.com>



Address.com

<http://www.address.com>



Zaba Search

<http://www.zabasearch.com>



Public People Finder

<http://www.publicpeoplefinder.com>



People Lookup

<https://www.peoplelookup.com>

FOOTPRINTING

Mọi người tìm kiếm trên dịch vụ mạng xã hội



<http://www.orkut.com>



<http://www.facebook.com>



<http://www.linkedin.com>



<http://twitter.com>

FOOTPRINTING



Thu thập thông tin từ các dịch vụ tài chính



FOOTPRINTING



Footprinting thông qua trang web việc làm

bạn có thể thu thập một công ty có các chi tiết cơ sở hạ tầng từ các quảng cáo việc làm



- công việc yêu cầu
- hồ sơ cá nhân người lao động
- thông tin phần cứng
- phần mềm thông tin

Job ID
17123.6554870.6
42319173004

Location
Boca Raton, FL 33487

Job Status
IT/Software Development

[Apply Now](#)



Network Administrator, Active Directory, Citrix, Exchange

Job Description:

- Design and implement technical solutions on the Windows platform to support business requirements.
- Support existing Windows Infrastructure including: Active Directory 2003, SMS, SUS, Citrix Metaframe, SQL Server, SQL Clusters, Exchange 5.5, Exchange 2003, VM Ware, Veritas backup software, Account and server security, Disaster Recovery services, RAID technologies, and Fibre/SAN disk solutions.

Job Experience:

- 5 or more years experience working in IT implementing and supporting a global business
- Prior experience in supporting a global Windows server and Domain Infrastructure
- Experience implementing and supporting Active Directory, Citrix Metaframe, SQL Server, SQL Cluster, DNS, DHCP, WINS, and Exchange 2003 in an Enterprise environment
- Very strong systems troubleshooting skills
- Experience in providing 24-hour support to a global enterprise as part of an on-call rotation
- Effective interpersonal skills with the ability to be persuasive
- Other skills: Building Effective Teams, Action Oriented Peer Relationships, Customer Focus, Priority Setting, Problem Solving, and Business Acumen
- Bachelor's Degree or equivalent experience
- MCSE (2003) certification a plus, Citrix Certification a plus

FOOTPRINTING



Giám sát mục tiêu bằng cách sử dụng các cảnh báo

- Google cảnh báo là một dịch vụ nội dung giám sát tự động thông báo cho người dùng nội dung từ tin tức, web, blog, video và / hoặc các nhóm thảo luận phù hợp với các thuật ngữ tìm kiếm được lựa chọn bởi người sử dụng và được lưu trữ bởi các dịch vụ cảnh báo google
- Google cảnh báo giúp đỡ trong việc theo dõi tin tức phát triển và giữ hiện hành về một đối thủ cạnh tranh hoặc các ngành công nghiệp



GigaAlert Generate Leads. Monitor Competitors. Safeguard Your Reputation.

Track your interests on the Web.

[Sign Up](#) [Log In](#)

The web's leading solution for maintaining your professional interests online. Track the entire web for your topics and receive new results by daily email.

© 2010 Intelligeant Technologies, provider of GigaAlert. GigaAlert may form a trademark or service mark. Terms of use

Login About Products Testimonials Press



Google alerts beta

Search terms: [Preview results](#)

Type:

How often:

Email length:

Your email:

[Create Alert](#)

FOOTPRINTING



Phương thức Footprinting



Internet
Footprinting



Competitive
Intelligence



WHOIS
Footprinting



DNS
Footprinting



Network
Footprinting



Website
Footprinting



E-mail
Footprinting



Google
Hacking



FOOTPRINTING



Cạnh tranh thông minh thu thập

Kinh doanh di chuyển nhanh. Chu kỳ sản phẩm được xác định trong tháng, không phải là năm. Các đối tác trở thành đối thủ nhanh hơn so với bạn có thể nói vi phạm hợp đồng. Vì vậy, làm thế nào có thể bạn có thể hy vọng để theo kịp với các đối thủ cạnh tranh của bạn nếu bạn không thể giám sát chúng.



Các thông tin tình báo cạnh tranh là không can thiệp và tinh tế về bản chất

Tình báo cạnh tranh có quá trình xác định, việc thu thập, phân tích, xác minh và sử dụng thông tin về các đối thủ cạnh tranh từ các nguồn tài nguyên như

FOOTPRINTING



Cạnh tranh thông minh thu thập

1

Sản phẩm công ty của bạn với đối thủ cạnh tranh là cung cấp



2

phân tích những vị trí thị trường của bạn so với các đối thủ cạnh tranh



3

kéo lên một danh sách các công ty cạnh tranh trên thị trường



4

Thu thập các câu chuyện chiến tranh từ người bán hàng làm thế nào giao dịch có thắng và thua trong lĩnh vực cạnh tranh



5

Tạo ra một hồ sơ cá nhân của giám đốc điều hành và quản lý toàn bộ nhân viên của đối thủ cạnh tranh



FOOTPRINTING



Cạnh tranh thông minh Khi nào các công ty bắt đầu,
Nó phát triển như thế nào?



Visit These Sites

01. EDGAR Database

<http://www.sec.gov/edgar.shtml>

02. Hoovers

<http://www.hoovers.com>

03. LexisNexis

<http://www.lexisnexis.com>

04. Dun & Bradstreet

<http://www.dnb.com>

FOOTPRINTING

Cạnh tranh thông minh Kế hoạch của các công ty là gì?



ABI/INFORM Global (<http://www.proquest.com>)



Factiva (<http://factiva.com>)



Business Wire (<http://www.businesswire.com>)



Market Watch (<http://www.marketwatch.com>)



Websitez (<http://websitez.com>)

FOOTPRINTING



FOOTPRINTING



Công cụ của cạnh tranh thông minh



Thông tin SEC
<http://www.secinfo.com>



C-SPAN
<http://www.cspan.org>



Tiền bối ra cho các
công ty nghiên cứu
<http://money.cnn.com>



Forbes 500
<http://www.forbes.com>



đường dây kinh doanh
<http://home.businesswire.com>



ChoicePoint Online
<http://www.choicepointonline.com>



Web điều tra
<http://www.web-investigator.net>



Barrons
<http://online.barrons.com>

FOOTPRINTING

Các công ty tư vấn cạnh tranh thông minh



The screenshot shows the Carratu website homepage. The header features the company name 'CARRATU' and a sub-header 'INVESTIGATIVE INTELLIGENCE'. Below the header, there's a banner with the text 'the only investigations company with a team dedicated entirely to the pharmaceutical world.' and an image of laboratory glassware. The main content area includes sections for 'CORPORATE INVESTIGATIONS', 'POLITICAL INVESTIGATIONS', 'INTELLECTUAL PROPERTY PROTECTION SERVICES', and 'IT FORENSICS & E-CRIME'. A sidebar on the left lists 'Welcome to Carratu', 'Investigative Services', and 'Case Studies'. A footer at the bottom contains links for 'HOME', 'SERVICES', 'CASE STUDIES', 'CONTACT US', 'MEDIA CENTER', and 'CALL 1-800-555-1234'.

<http://www.carratu.com>



The screenshot shows the Fuld & Company website homepage. The header features the company name 'FULD & COMPANY' and a sub-header 'The Global Leader in Competitive Intelligence'. Below the header, there are several sections: 'Business & Analytics & Related Services', 'Industry Practices', 'Intelligence Indexes & Reference Center', and a quote from Paul Gompert: 'The indispensable basis of competitive intelligence'. A sidebar on the left lists 'About Fuld' and 'THE SECRET LIFE OF COMPETITIVE INTELLIGENCE'. A footer at the bottom contains links for 'HOME', 'SERVICES', 'DRIVE', 'SUBSCRIPTIONS', 'TERMS & CONDITIONS', and 'How to subscribe through...

<http://www.fuld.com>



The screenshot shows the Global Intelligence Alliance website homepage. The header features the company name 'Global Intelligence Alliance'. Below the header, there's a banner with the text 'Partner with us to understand, compete and grow in international markets'. The main content area includes sections for 'Strategic Market Intelligence & Analytics', 'Market Research Services', 'Competitor Analysis', 'Geopolitical Risk', and 'Intelligence Network'. A sidebar on the left lists 'Overall Risk Categories' and 'Geopolitical Risk'. A footer at the bottom contains links for 'HOME', 'ABOUT', 'SERVICES', 'RESOURCES', 'CONTACT', and 'LOG IN'.

<http://www.globalintelligence.com>



The screenshot shows the Datamonitor website homepage. The header features the company name 'DATAMONITOR' and a sub-header 'the leader in Business Information'. Below the header, there's a banner with the text 'Size and segment the logistics market with: Global Logistics and Express Analyzer'. The main content area includes sections for 'Browse and purchase our research', 'RESEARCH STORE', 'Access our premium subscription services', 'KNOWLEDGE CENTER', and 'Get competitive insight and consulting services'. A sidebar on the left lists 'Overall Risk Categories' and 'Geopolitical Risk'. A footer at the bottom contains links for 'HOME', 'ABOUT', 'SERVICES', 'RESOURCES', 'CONTACT', and 'LOG IN'.

<http://www.datamonitor.com>



FOOTPRINTING

Phương thức Footprinting



FOOTPRINTING



Whois tra cứu

Cơ sở dữ liệu whois được duy trì bởi vùng đăng ký mạng Internet và chứa các thông tin cá nhân của các chủ tên miền

Công cụ Whois tra cứu

<http://www.tamos.com>
<http://netcraft.com>
<http://www.whois.net>
<http://www.ip-tools.com>

- whois câu truy vấn trả lại
1. tên miền chi tiết
 2. chi tiết liên lạc của chủ sở hữu tên miền
 3. tên miền máy chủ
 4. NetRange(phạm vi)



vùng mạng Internet đăng ký

1. AfriNIC
2. ARIN
3. APNIC
4. LACNIC, RIPE NCC



kẻ tấn công tìm kiếm

1. vật lý vị trí
2. số điện thoại
3. địa chỉ email
4. kỹ thuật và hành chính liên lạc



FOOTPRINTING



Whois tra tìm kết quả phân tích

Registrant:
targetcompany (targetcompany-DOM)
133 Avenue Elik A. Enciso
American
Hypermail
auto-scales.com, SOC0001
DE
Domain Name: targetcompany.COM

Administrative Contact:
*****, 2444 (03322-080) targetcompany@D1.VSMC.VN
targetcompany
133, Avenue Elik A. Enciso,
American
Hypermail, Auto-scales.com, SOC0001
DE 91 40 XXXX 3248 Fax: 91 40 XXXX 3248
Technical Contact:
*****, YYYY (0332) techcontact@WEBHOST.COM
XXXX, DE
Domain Name: targetcompany.COM
Record expires on 14-Oct-2002.
Record created on 13-Oct-1997.
Database last updated on 13-May-2001 07:49:04 EST.

Domain servers in listed order:
NS1.WEBHOST.COM 294.XXX.148.201
NS2.WEBHOST.COM 294.XXX.141.201

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX
Technical Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:

NS1.WEBHOST.COM	XXX.XXX.XXX.XXX
NS2.WEBHOST.COM	XXX.XXX.XXX.XXX

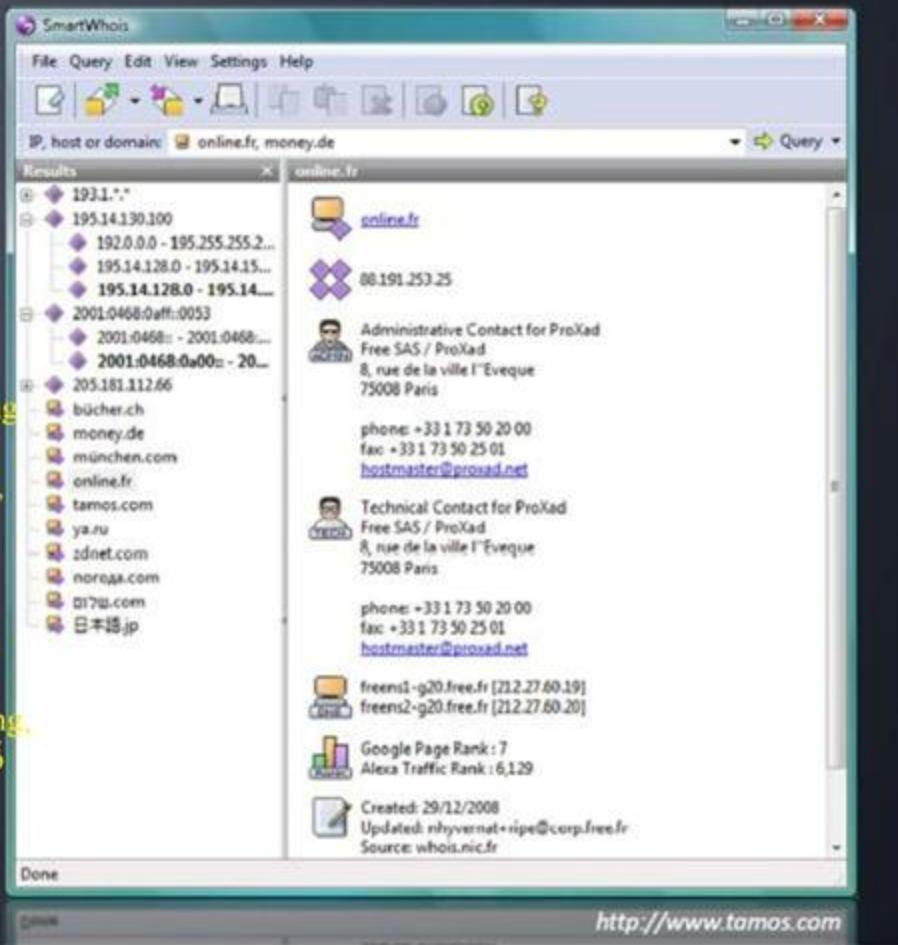
FOOTPRINTING

Công cụ whois tra cứu

SmartWhois

SmartWhois là một tiện ích mạng có những thông tin hữu ích cho phép bạn nhìn về một địa chỉ IP, tên máy hoặc tên miền

Nó cũng cung cấp thông tin về đất nước, nhà nước hoặc tỉnh, thành phố, tên của các nhà cung cấp mạng, quản trị, và thông tin hợp đồng hỗ trợ kỹ thuật



FOOTPRINTING



Công cụ Whois tìm kiếm



Sam Spade

<http://samspade.org>



My IP Suite

<http://www.sabsoft.com>



CountryWhois

<http://www.tamos.com>



LanWhois

<http://lantricks.com>



NetRanger Whois

<http://www.conceiva.com>



Lapshins Whois

<http://lapshins.com>



Alchemy Eye

<http://www.alchemy-lab.com>



WebFerret

<http://www.webferret.com>

FOOTPRINTING



Công cụ Whois tra cứu trực tuyến



Whois

<http://tools.whois.net>



Whois Lookup

<http://www.ip-tools.com>



Better Whois

<http://www.betterwhois.com>



Geek Whois

<http://www.geektools.com>



Arin Whois Database Search

<http://whois.arin.net>



Network Solutions Whois

<http://www.networksolutions.com>



DomainTools

<http://www.domaintools.com>



AutoWhois

<http://centralops.net>

FOOTPRINTING



Footprinting Methodology

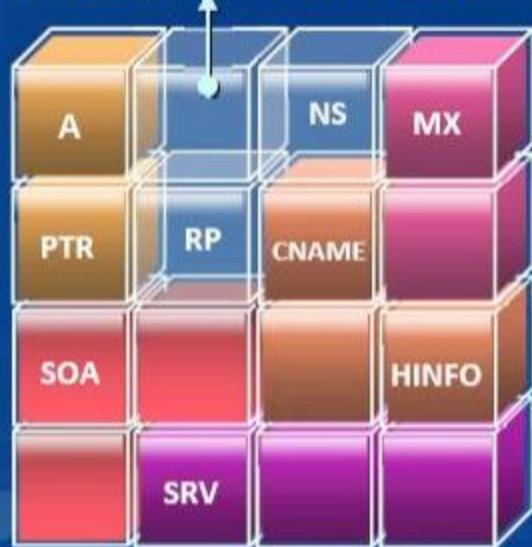


FOOTPRINTING



Thông tin giải nén của DNS

Kiểu ghi của DNS



Bảng ghi DNS cung cấp thông tin quan trọng về những vị trí và loại máy chủ

-  **A** - Trỏ đến một địa chỉ IP host
-  **MX** - Trỏ đến tên miền của máy chủ mail
-  **NS** - Trỏ đến tên miền của máy chủ
-  **CNAME** - Quy tắc đặt tên cho một máy chủ
-  **SOA** - Cho biết ý nghĩa của một tên miền
-  **SRV** - Thông tin của một dịch vụ
-  **PTR** - Giả mạo địa chỉ IP của một máy chủ
-  **RP** - Người chịu trách nhiệm
-  **HINFO** - Các máy chủ lưu trữ thông tin bao gồm CPU và OS

**DNS
Interrogation
Tools**

-  <http://www.dnsstuff.com>
-  <http://www.checkdns.net>

-  <http://network-tools.com>
-  <http://www.ip-tools.com>

FOOTPRINTING

Thông tin từ DNS

CheckDNS.NET is testing microsoft.com

CheckDNS.NET is asking root servers about authoritative NS for domain

Got DNS list for 'microsoft.com' from e.gtld-servers.net or e.gtld-servers.net or e.gtld-servers.net or e.gtld-servers.net or e.gtld-servers.net

- ❶ Found NS record: ns1.msft.net[65.55.37.62], was resolved to IP address by e.gtld-servers.net ⓘ
- ❷ Found NS record: ns2.msft.net[64.4.59.173], was resolved to IP address by e.gtld-servers.net ⓘ
- ❸ Found NS record: ns3.msft.net[213.199.161.77], was resolved to IP address by e.gtld-servers.net ⓘ
- ❹ Found NS record: ns4.msft.net[207.46.75.254], was resolved to IP address by e.gtld-servers.net ⓘ
- ❺ Found NS record: ns5.msft.net[65.55.226.140], was resolved to IP address by e.gtld-servers.net ⓘ
- Domain has 5 DNS server(s) ⓘ

CheckDNS.NET is verifying if NS are alive

- ❶ DNS server ns1.msft.net[65.55.37.62] is alive and authoritative for domain microsoft.com ⓘ
- ❷ DNS server ns2.msft.net[64.4.59.173] is alive and authoritative for domain microsoft.com ⓘ
- ❸ DNS server ns3.msft.net[213.199.161.77] is alive and authoritative for domain microsoft.com ⓘ
- ❹ DNS server ns4.msft.net[207.46.75.254] is alive and authoritative for domain microsoft.com ⓘ
- ❺ DNS server ns5.msft.net[65.55.226.140] is alive and authoritative for domain microsoft.com ⓘ
- 5 server(s) are alive ⓘ

CheckDNS.NET checks if all NS have the same version

- All 5 your servers have the same zone version 2010070903 ⓘ

FOOTPRINTING

Các công cụ kiểm tra DNS



NetInspector
<http://www.globware.com>



NSLOOKUP
<http://www.kloth.net>



DigDug, DNS Analyzer
<http://www.edge-security.com>



MSR Strider URL Tracer
<http://research.microsoft.com>



WhereISIP
<http://www.whereisip.com>



Dnsmap
<http://www.linuxhaxor.net>



Multiple Addresses
<http://www.checkdns.net>



DNS Tool
<http://www.hendricom.com>

FOOTPRINTING

Các công cụ kiểm tra DNS trực tuyến



Online DNS Tools

<http://www.ajaxdns.com>



Better Whois

<http://www.betterwhois.com>



Professional Toolset

<http://www.dnsstuff.com>



Geek Whois

<http://www.geektools.com>



DNS Record

<http://network-tools.com>



Mozzle Domain Name Pro

<http://www.mozzle.com>



Check DNS

<http://www.checkdns.net>



Domain Information Groper

<http://www.kloth.net>

FOOTPRINTING

Quá trình footprinting



FOOTPRINTING



xác định vị trí

Phạm vi của mạng

1. Phạm vi của địa chỉ IP ,
2. Sử dụng công cụ tìm kiếm dữ liệu ARIN whois

Bạn cần dãy địa chỉ IP

Network Whois record

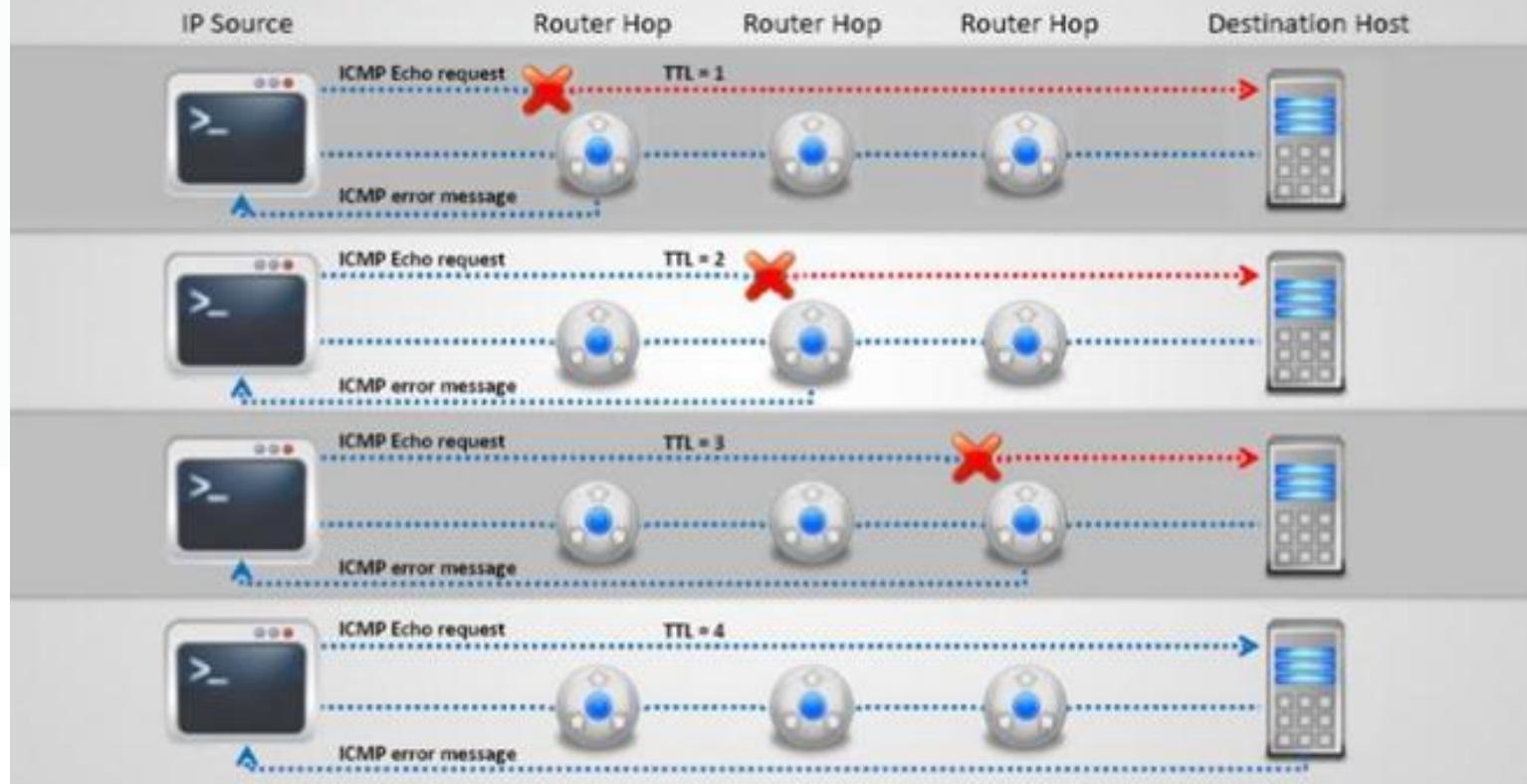
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:	207.46.0.0 - 207.46.255.255
CIDR:	207.46.0.0/16
OriginAS:	
NetName:	MICROSOFT-GLOBAL-NET
NetHandle:	NET-207-46-0-0-1
Parent:	NET-207-0-0-0-0
NetType:	Direct Assignment
NameServer:	NS2.MSFT.NET
NameServer:	NS4.MSFT.NET
NameServer:	NS1.MSFT.NET
NameServer:	NS5.MSFT.NET
NameServer:	NS3.MSFT.NET
RegDate:	1997-03-31
Updated:	2004-12-09
Ref:	http://whois.arin.net/rest/net/NET-207-46-0-0-1
OrgName:	Microsoft Corp
OrgId:	MSFT
Address:	One Microsoft Way
City:	Redmond
StateProv:	WA
PostalCode:	98052
Country:	US
RegDate:	1998-07-10
Updated:	2009-11-10
Ref:	http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle:	ABUSE231-ARIN
OrgAbuseName:	Abuse

FOOTPRINTING

Chương trình Traceroute làm việc trên các khái niệm về giao thức ICMP và sử dụng trường TTL trong header của gói tin ICMP để khám phá các bộ định tuyến đường đi đến các máy chủ mục tiêu.

Traceroute



FOOTPRINTING



Phân tích chương trình Traceroute

I

Những kẻ tấn công bằng Traceroute để lấy thông tin về: cấu trúc liên kết mạng, thiết bị định tuyến, và tường lửa

II

Ví dụ: sau khi chạy Traceroute thì người tấn công có thể có được các thông tin sau:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.12
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

III

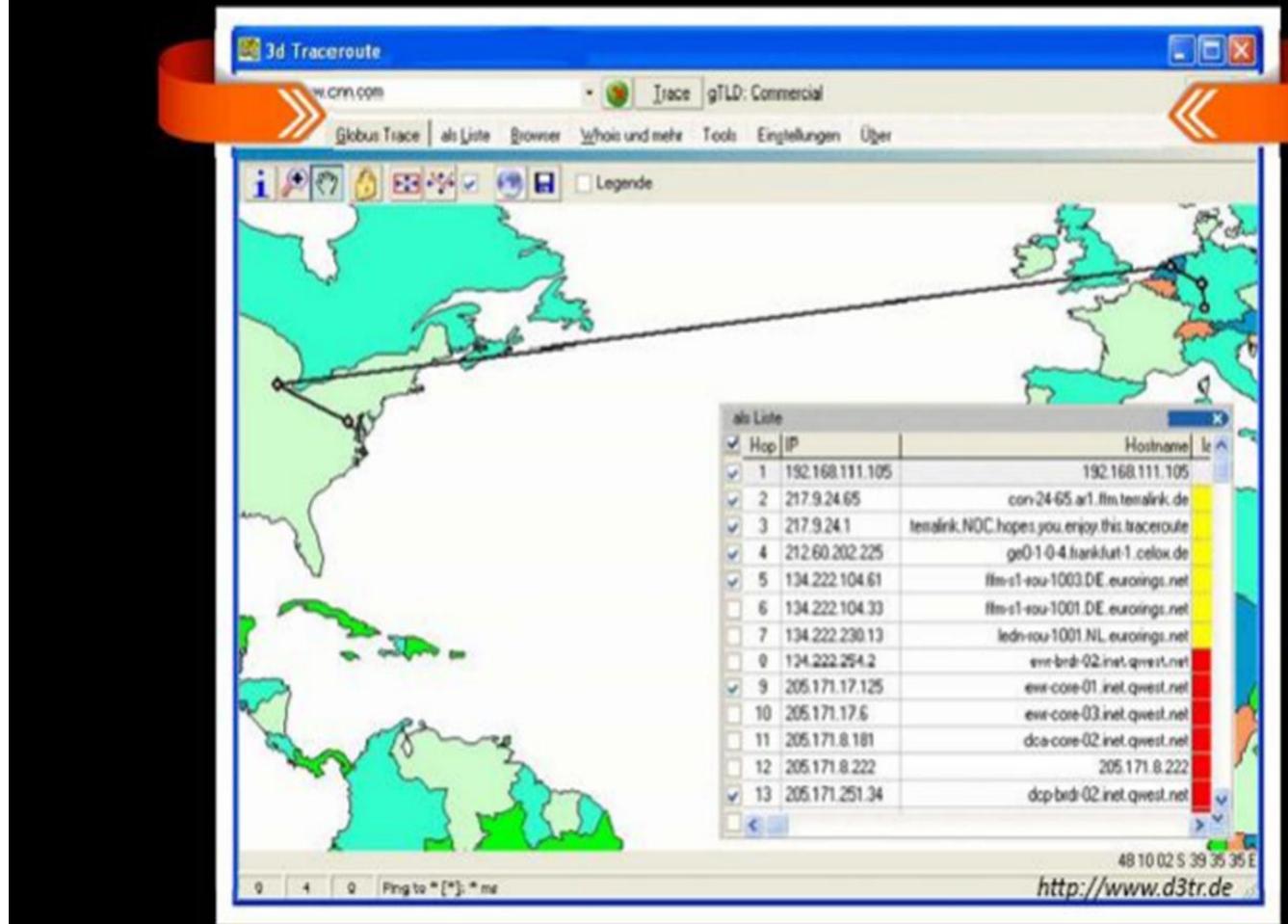
Bằng cách đưa thông tin này lại với nhau, kẻ tấn công có thể vẽ sơ đồ mạng



FOOTPRINTING

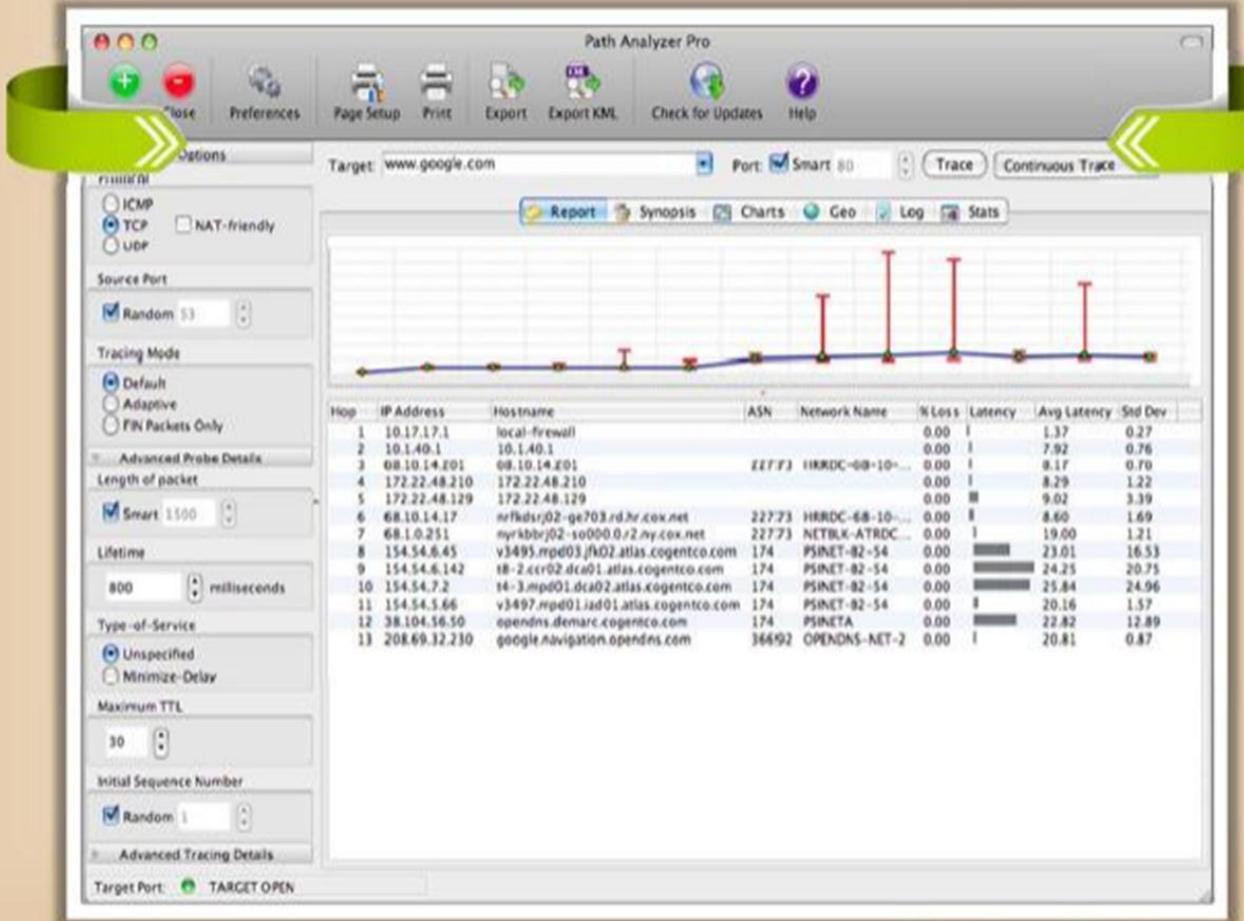


Công cụ Traceroute: Traceroute 3D



FOOTPRINTING

Công cụ Traceroute: Path Analyzer Pro



FOOTPRINTING



Công cụ Traceroute



VisualRoute Trace

<http://visualroute.visualware.com>



GEOSpider

<http://www.oreware.com>



vTrace

<http://vtrace.pl>



Magic NetTrace

<http://www.tialsoft.com>



3d Visual Trace Route

<http://www.3dsnmp.com>



Visual IP Trace

<http://www.visualiptrace.com>



Trout

<http://www.foundstone.com>



Patrice Zwenger Traceroute

<http://patrice-zwenger.co.cc>

FOOTPRINTING

Các công cụ Traceroute



AnalogX HyperTrace

<http://www.analogx.com>



Layer Four Traceroute

<http://pwhois.org>



Tcp Trace Route

<http://michael.toren.net>



Ping Plotter

<http://www.pingplotter.com>



Network Systems Traceroute

<http://www.net.princeton.edu>



Tracepath

<http://whatismyipaddress.com>



Roadkil's Trace Route

<http://www.roadkil.net>



Ping-Probe

<http://www.ping-probe.com>

FOOTPRINTING

Phương pháp Footprinting



FOOTPRINTING

Phản ánh toàn bộ trang web

Web công cụ cho phép bạn tải về một trang web vào một thư mục cục bộ, xây dựng lặp tất cả các thư mục, HTML, hình ảnh, flash, video và các file khác từ máy chủ đến máy tính của bạn



Original Website

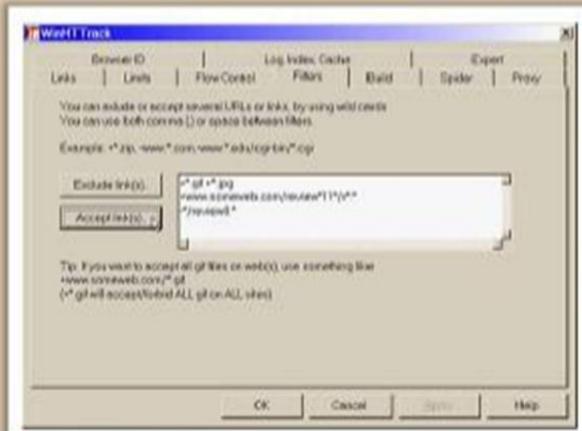
Mirrored Website



FOOTPRINTING



Công cụ là trang web của Mirroring



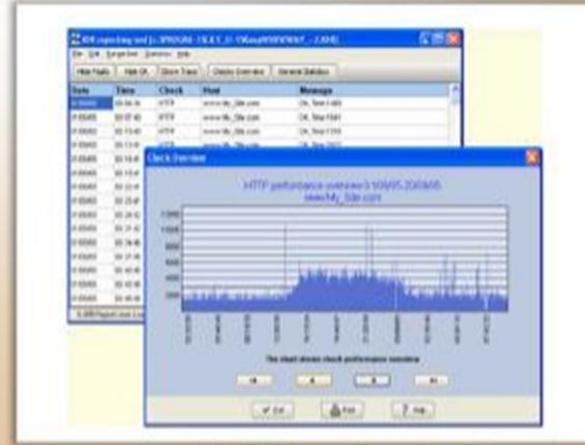
HTTrack Web Site Copier (<http://www.httrack.com>)



SurfOffline (<http://www.surfoffline.com>)



PageNest (<http://www.pagenest.com>)



KeepNI (<http://www.keepni.com>)

FOOTPRINTING



Trang web Mirrorinc toàn bộ công cụ



Wget

<http://www.gnu.org>



Website Ripper Copier

<http://www.tensons.com>



Webripper

<http://calluna-software.com>



BlackWidow

<http://softbytelabs.com>



WinWS

<http://winwsd.uw.hu>



Reamweaver

<http://reamweaver.com>



xaldon webspider 2

<http://www.xaldon.de>



Teleport Pro

<http://www.tenmax.com>

FOOTPRINTING



VD: Bảng thông tin của trang web
<http://www.archive.org>

INTERNET ARCHIVE
WayBack Machine

Internet Archive Wayback Machine allows you to visit archived versions of Web sites

Enter Web Address: <http://www.microsoft.com> All Take Me Back Adv. Search Compare Archive Pages

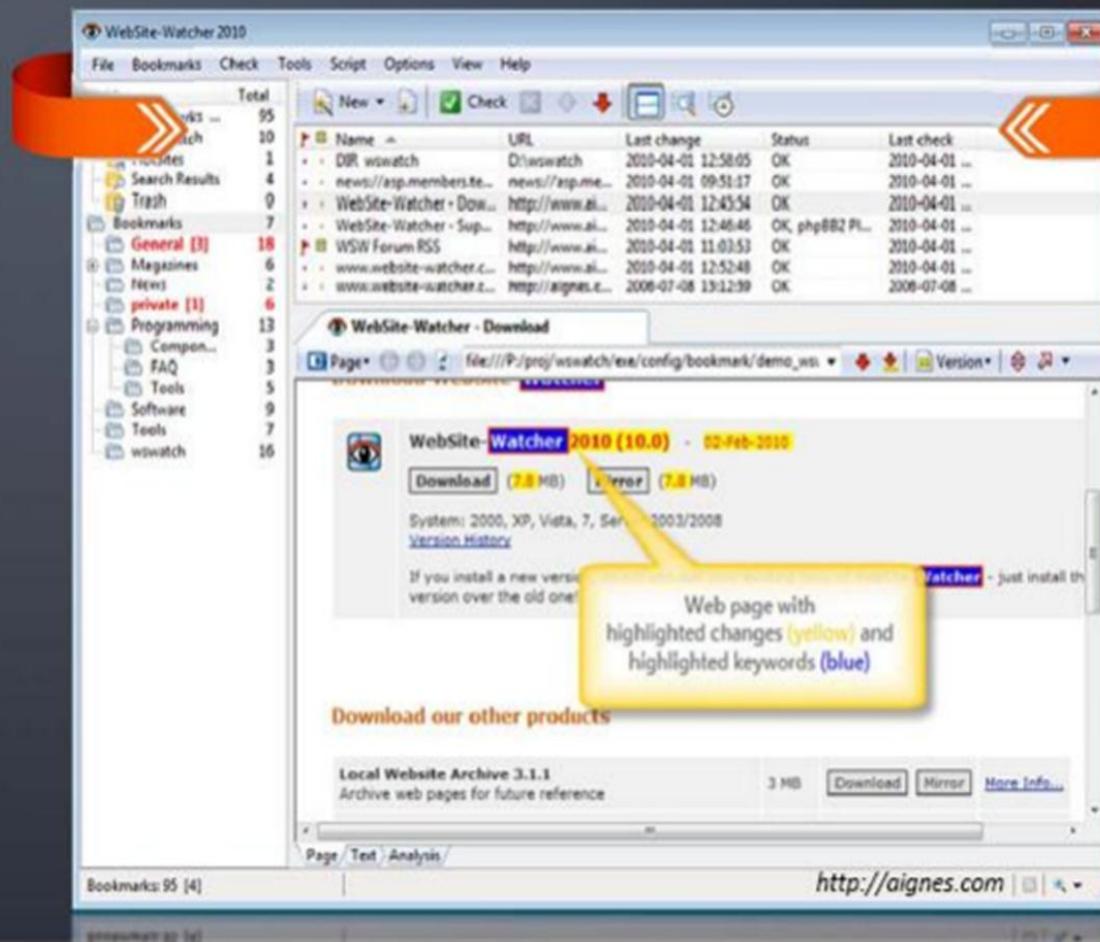
Searched for <http://www.microsoft.com>

Archived Results from Jan 01, 1996 - latest

2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
263 pages	139 pages	30 pages	169 pages	375 pages	278 pages	209 pages	133 pages	7 pages	1 pages
Jan 03, 2001	Jan 21, 2002	Jan 30, 2003	Jan 10, 2004	Jan 04, 2005	Jan 01, 2006	Jan 02, 2007	Jan 01, 2008	Jul 23, 2009	Feb 23, 2010
Jan 03, 2001	Jan 25, 2002	Feb 08, 2003	Jan 17, 2004	Jan 10, 2005	Jan 01, 2006	Jan 03, 2007	Jan 02, 2008	Jul 23, 2009	
Jan 04, 2001	Jan 27, 2002	Feb 20, 2003	Jan 24, 2004	Jan 14, 2005	Jan 01, 2006	Jan 07, 2007	Jan 03, 2008	Oct 18, 2009	
Jan 05, 2001	Jun 03, 2002	Mar 21, 2003	Feb 02, 2004	Jan 15, 2005	Jan 01, 2006	Jan 07, 2007	Jan 04, 2008	Oct 18, 2009	
Jan 06, 2001	Jun 04, 2002	Mar 24, 2003	Feb 07, 2004	Jan 16, 2005	Jan 01, 2006	Jan 08, 2007	Jan 04, 2008	Oct 26, 2009	
Jan 06, 2001	Jun 05, 2002	Mar 28, 2003	Feb 08, 2004	Jan 17, 2005	Jan 01, 2006	Jan 09, 2007	Jan 05, 2008	Oct 27, 2009	
Jan 07, 2001	Jul 01, 2002	Apr 11, 2003	Feb 09, 2004	Jan 18, 2005	Jan 02, 2006	Jan 12, 2007	Jan 06, 2008	Oct 27, 2009	
Jan 08, 2001	Jul 02, 2002	May 06, 2003	Feb 14, 2004	Jan 19, 2005	Jan 02, 2006	Jan 14, 2007	Jan 08, 2008		
Jan 08, 2001	Jul 03, 2002	May 13, 2003	Feb 21, 2004	Jan 20, 2005	Jan 02, 2006	Jan 17, 2007	Jan 09, 2008		
Jan 08, 2001	Jul 03, 2002	May 29, 2003	Feb 28, 2004	Jan 21, 2005	Jan 02, 2006	Jan 25, 2007	Jan 09, 2008		
Jan 08, 2001	Jul 04, 2002	Jun 18, 2003	Mar 06, 2004	Jan 22, 2005	Jan 02, 2006	Jan 26, 2007	Jan 10, 2008		
Jan 18, 2001	Jul 07, 2002	Jun 18, 2003	Mar 13, 2004	Jan 23, 2005	Jan 03, 2006	Jan 28, 2007	Jan 10, 2008		
Jan 18, 2001	Jul 08, 2002	Jun 23, 2003	Mar 25, 2004	Jan 24, 2005	Jan 03, 2006	Jan 29, 2007	Jan 11, 2008		
Jan 30, 2001	Jul 09, 2002	Jun 24, 2003	Apr 01, 2004	Jan 25, 2005	Jan 03, 2006	Jan 30, 2007	Jan 12, 2008		
Feb 02, 2001	Jul 11, 2002	Jul 17, 2003	Apr 10, 2004	Jan 26, 2005	Jan 04, 2006	Feb 01, 2007	Jan 17, 2008		
Feb 02, 2001	Jul 12, 2002	Aug 05, 2003	Apr 15, 2004	Jan 27, 2005	Jan 04, 2006	Feb 02, 2007	Jan 18, 2008		
Feb 24, 2001	Jul 13, 2002	Aug 07, 2003	Apr 18, 2004	Jan 29, 2005	Jan 04, 2006	Feb 02, 2007	Jan 19, 2008		
Feb 28, 2001	Jul 14, 2002	Sep 25, 2003	May 18, 2004	Jan 29, 2005	Jan 05, 2006	Feb 03, 2007	Jan 19, 2008		
Mar 01, 2001	Jul 15, 2002	Oct 01, 2003	May 22, 2004	Jan 30, 2005	Jan 05, 2006	Feb 04, 2007	Jan 21, 2008		

FOOTPRINTING

Theo dõi thông tin cập nhật Web sử dụng trang web Watcher



FOOTPRINTING

Quá trình Footprinting



FOOTPRINTING

Theo dõi Email truyền thông

Theo dõi e-mail là một phương pháp để theo dõi và dò thám gửi e-mail tới người nhận

- | | |
|----|---|
| 01 | Khi email được nhận và đọc |
| 02 | Gởi emails phá hoại |
| 03 | gps vị trí và bản đồ ở người |
| 04 | Thời gian đọc email |
| 05 | Có hoặc không người nhận truy cập |
| 06 | Từng loại pdf và các tập tin đính kèm |
| 07 | đặt tin nhắn hết hạn sau một thời gian quy định |

Email
Tracking



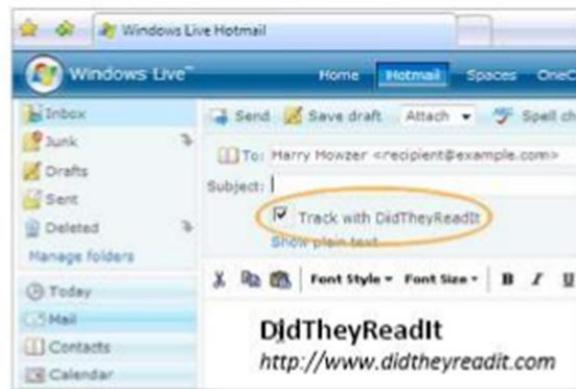
FOOTPRINTING



Email Tracking Tools



Read Notify
<http://www.readnotify.com>



PoliteMail
<http://www.politemail.com>



FOOTPRINTING

Email là công cụ theo dõi



VisualRoute Trace

<http://visualroute.visualware.com>



vTrace

<http://vtrace.pl>



3d Visual Trace Route

<http://www.3dsnmp.com>



Trout

<http://www.foundstone.com>



GEOSpider

<http://www.oreware.com>



Magic NetTrace

<http://www.tialsoft.com>



Visual IP Trace

<http://www.visualiptrace.com>



Patrice Zwenger Traceroute

<http://patrice-zwenger.co.cc>

FOOTPRINTING

Quá trình Footprinting



FOOTPRINTING



Footprinting sử dụng kỹ thuật Google Hacking

Truy vấn chuỗi

Google hacking là một thuật ngữ dùng để chỉ nghệ thuật tạo ra các công cụ truy vấn tìm kiếm phức tạp



Trang web vulnerable

Phát hiện các trang web dễ bị xâm nhập để khai thác và các lỗ hổng



Google là nhà điều hành

Nó sử dụng google để khai thác xác định vị trí của các chìu cù thế



FOOTPRINTING



Một Hacker có thể làm gì với Google Hacking?



FOOTPRINTING



Tìm Tài nguyên bằng cách sử dụng Google

[intitle: mạng nội bộ inurl: mạng nội bộ + intext: "nguồn nhân lực"]:

Nó cho phép bạn không chỉ để truy cập vào mạng riêng của công ty, mà còn cung cấp danh sách các nhân viên và các thông tin nhạy cảm khác có thể là vô cùng hữu ích cho bất kỳ nỗ lực kỹ thuật xã hội



Google™

Web Images Videos Maps News Shopping Gmail more ▾ Sign in

intitle:intranet inurl:intranet +intext:"human reso" Search Advanced Search Preferences

Web Show options... Results 1 - 10 of about 49,800 for intitle:intranet inurl:intranet +inte

[Intranet - Human Resources](#) Inside the Office of Commissioner of Higher Education.
[/che/intranet/hr.htm](#) - Cached - Similar

[Department of Personnel - Intranet Center](#) The Department of Human Resources Intranet is only available to people on the GOVnet network. This can be by direct connection, or through dial up directly ...
[/intranet/index.php](#) - Cached - Similar

[Intranet Site](#) 11 Jun 2009 ... Human Resources & Organizational Effectiveness - HROE ... recruitment and hiring, **human resources** and employee relations, compensation and ...
[intranet.library.](#) - Cached - Similar

[Colorado Intranet Human Resources](#) Colorado Intranet: **Human Resources**. Employee Benefits and Resources. Ag Learn provides education services for USDA employees, contractors, partners, ...
[intranet/personnel/perps.htm](#) - Similar



FOOTPRINTING



Hacking Công cụ của Google: Google Hacking cơ sở dữ liệu (GHDB)

The screenshot shows the homepage of Hackers For Charity.org with a focus on the GHDB (Google Hacking Database). The page has a dark orange header with a blue ribbon banner containing the text "HACKERS FOR CHARITY.ORG". Below the banner, there's a quote: "I'm Johnny. I Hack Stuff." The main menu includes links for Home, Hackers For Charity, Johnny, Get Involved, Informer, and GHDB. The GHDB section features a welcome message about the database, sections for Advisories and Vulnerabilities, Error Messages, and Files containing juicy info, and a link to the full database at <http://www.hackersforcharity.org>. A sidebar on the right lists a "Donor Cloud" with names like Barbara Ventzke, Chris John Riley, dandies.org, hardly, Kinderabsicherung, Krawiklett LVM Oranienburg, McLovin, Nathan Penetration Testing Scott, E Christiansen, skipper, Ventzke & Partner, Webdesign Webdesign Berlin, and NE GENERATOR.

"I'm Johnny. I Hack Stuff."

Home Where it all began

Hackers For Charity Seriously?

Johnny He hacks stuff.

Get Involved Do Something

Informer Go Backstage

GHDB Google Hacking Central

GHDB

Welcome to the Google Hacking Database (GHDB)!
We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!

Advisories and Vulnerabilities (215 entries)
These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Error Messages (68 entries)
Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)
No usernames or passwords, but interesting stuff none the less.

http://www.hackersforcharity.org

Donate, get linked, feed a child.
All proceeds go directly to our Kenya food for work project.

Barbara Ventzke Chris John Riley
dandies.org hardly Kinderabsicherung
Krawiklett LVM Oranienburg McLovin
Nathan Penetration Testing Scott
E Christiansen skipper Ventzke &
Partner, Webdesign Webdesign Berlin,
NE GENERATOR

FOOTPRINTING



Công cụ hacking Google



MetaGoofil
<http://www.edge-security.com>



Goolink Scanner
<http://www.ghacks.net>



SiteDigger
<http://www.foundstone.com>



Google Hacks
<http://code.google.com>



Google Cartography
<http://richard.jones.name>



Google Hack Honeypot
<http://ghh.sourceforge.net>



GMapCatcher
<http://code.google.com>



BiLE Suite
<http://www.sensepost.com>

FOOTPRINTING



Module lưu lượng



Footprinting
Khái niệm



Footprinting
Mối đe dọa



Footprinting
Phương pháp



Footprinting
Công cụ



Footprinting
Biện pháp đối phó



Footprinting
Bút thử nghiệm

FOOTPRINTING

Các công cụ Footprinting



Prefix Whois

<http://pwwhois.org>



NetScanTools Pro

<http://www.netscantools.com>



**DMitry (Deepmagic
Information Gathering Tool)**

<http://www.mor-pah.net>



Netmask

<http://www.phenoelit-us.org>



Tctrace

<http://www.phenoelit-us.org>



Maltego

<http://www.paterva.com>



**Autonomous System
Scanner(ASS)**

<http://www.phenoelit-us.org>



Host

<http://linux.die.net>

FOOTPRINTING

Các công cụ Footprinting



DNS DIGGER
<http://www.dnsdigger.com>



Domain Name Analyzer
<http://www.domainpunch.com>



Dig Web Interface
<http://www.digwebinterface.com>



Trellian
<http://ci.trellian.com>



Domain Research Tool (DRT)
<http://www.domainresearchtool.com>



Spiderzilla
<http://spiderzilla.mozilla.org>



DomainInspect
<http://www.antsoft.com>



Compete
<http://searchanalytics.compete.com>

FOOTPRINTING

Các công cụ Footprinting



Touchgraph
<http://www.touchgraph.com>



ActiveWhois
<http://www.johnru.com>



theHarvester
<http://www.edge-security.com>



Advanced Administrative Tool
<http://www.glocksoft.com>



Spyfu
<http://www.spyfu.com>



Subdomainer
<http://www.edge-security.com>



CallerIP
<http://www.callerippro.com>



Alchemy Network Tool
<http://www.alchemy-lab.com>

FOOTPRINTING



Module lưu lượng



Khái niệm
Footprinting



Các mối đe dọa của
việc Footprinting



Phương pháp
Footprinting



Công cụ Footprinting



Các biện pháp đối phó
Footprinting



Bút kiểm tra
Footprinting

FOOTPRINTING



Biện pháp đối phó Footprinting

1. Cấu hình bộ định tuyến để hạn chế các yêu cầu footprinting
2. Cấu hình máy chủ web để tránh rò rỉ thông tin và vô hiệu hóa các giao thức không mong muốn
3. Khóa các cổng với cấu hình tường lửa phù hợp
4. Sử dụng một IDS có thể được cấu hình để từ chối lưu lượng truy cập nghi ngờ và lấy mẫu footprinting
5. Kiểm tra thông tin trước khi đưa lên web / Internet
6. Thực hiện kỹ thuật footprinting và loại bỏ bất kỳ thông tin nhạy cảm được tìm thấy
7. Ngăn chặn các công cụ tìm kiếm từ bộ nhớ đệm một trang web và đăng ký sử dụng dịch vụ ẩn
8. Vô hiệu hóa các danh sách thư mục và sử dụng split-DNS

FOOTPRINTING



Bút kiểm tra Footprinting

- ∅ + Bút Footprinting được sử dụng để kiểm tra và xác định thông tin của tổ chức công bố công khai trên Internet như kiến trúc mạng, hệ điều hành, ứng dụng và người sử dụng
- + Kiểm tra để thu thập càng nhiều thông tin càng tốt về tổ chức mục tiêu từ internet và các nguồn truy cập công cộng khác

Ngăn chặn rò rỉ thông tin



Bút Footprinting
sẽ giúp quản trị viên
kiểm tra



Ngăn chặn các bảng
ghi đã có sẵn trong
DNS

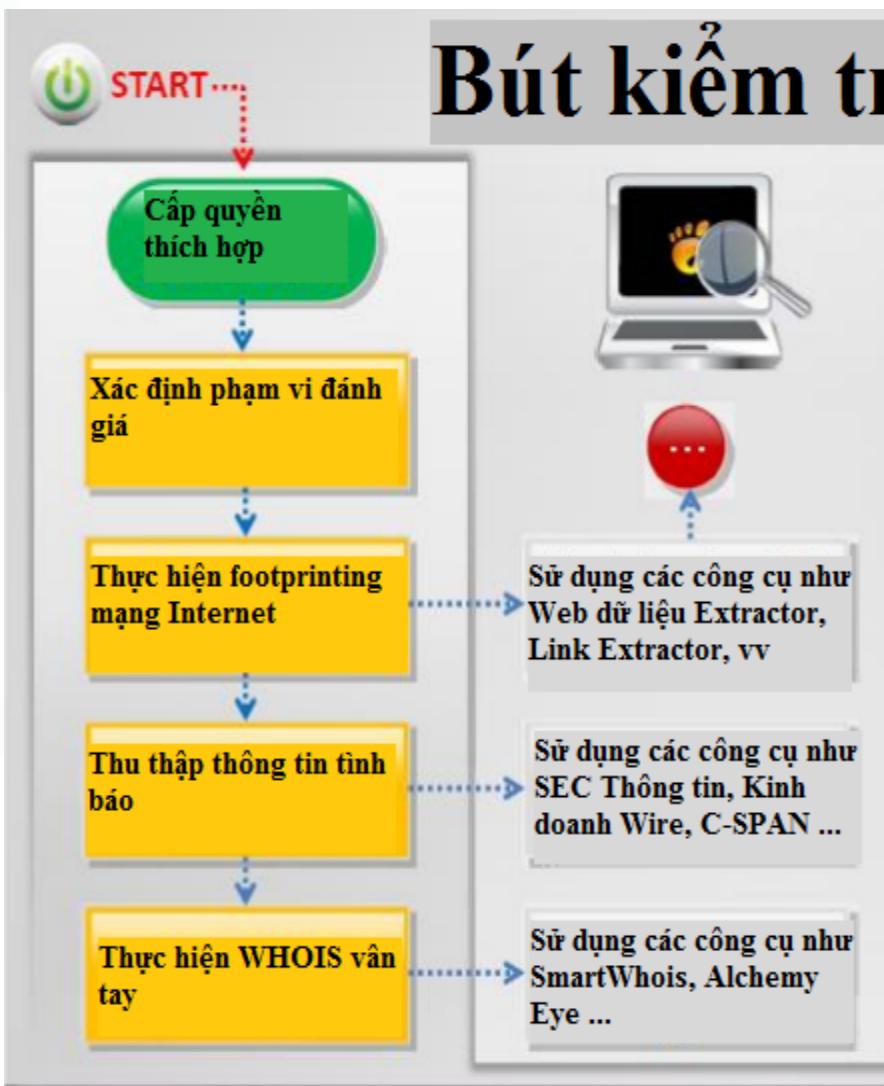


Ngăn chặn các kỹ thuật

FOOTPRINTING



Bút kiểm tra Footprinting



Nhận sự cho phép thích hợp và xác định phạm vi đánh giá

Thực hiện footprinting mạng Internet bằng cách sử dụng các công cụ như Web dữ liệu Extractor, Link Extractor ...

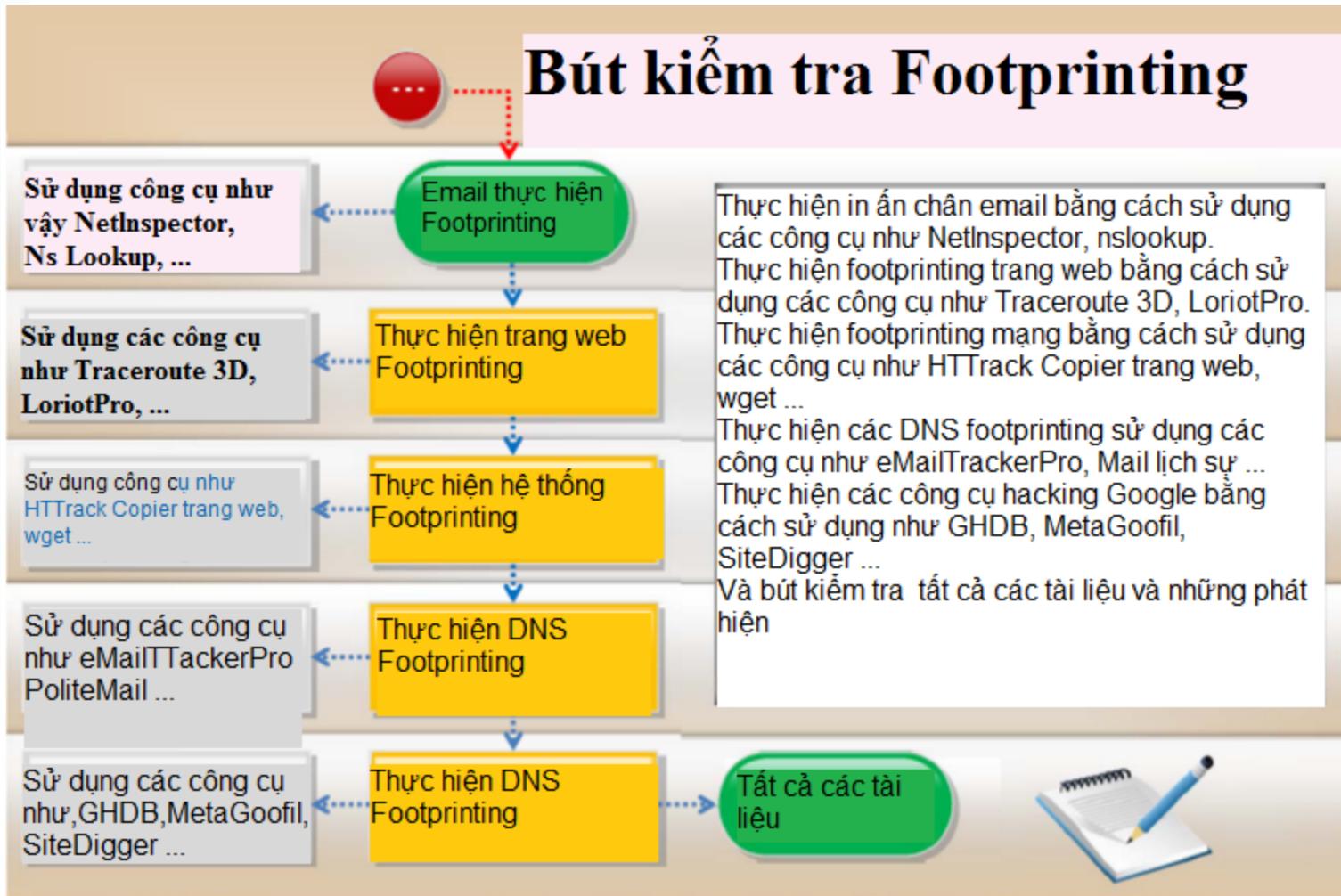
Thu thập thông tin tình báo cạnh tranh bằng cách sử dụng các công cụ như SEC Thông tin, dây kinh doanh, C-SPAN ...

Thực hiện WHOIS vân tay bằng cách sử dụng các công cụ như SmartWhois, Alchemy Eye ...

FOOTPRINTING



Bút kiểm tra Footprinting



FOOTPRINTING

Kết luận



- + Footprinting đề cập để phát hiện và thu thập thông tin càng nhiều càng tốt về một mục tiêu tấn công.
- + Cơ sở dữ liệu WHOIS được duy trì đăng ký qua mạng Internet khu vực và chứa các thông tin cá nhân của chủ sở hữu tên miền.
- + Ghi DNS cung cấp thông tin quan trọng về vị trí và loại máy chủ.
- + Thông tin cá nhân có thể được tìm thấy bằng cách sử dụng người dịch vụ tìm kiếm trực tuyến.
- + Bạn có thể thiết lập thông tin liên lạc email với công ty mục tiêu và theo dõi các email để trích xuất các thông tin như vị trí của các máy chủ người nhận và thư.
- + Thu thập thông tin tình báo cạnh tranh là quá trình thu thập thông tin về đối thủ cạnh tranh của bạn từ các nguồn tài nguyên chẳng hạn như Internet

Quotes

"Nếu bạn biết đối phương và biết chính mình, bạn không cần phải lo sợ kết quả của các cuộc tấn công."

- Sun Tzu,
Ancient Chinese
Strategist and
Philosopher