TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THÔNG TIN HỮU NGHỊ VIỆT HÀN

KHOA: KHOA HỌC MÁY TÍNH

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.

C|EH™

Certified Ethical Hacker

FOOTPRINTING

BẢO MẬT TIN TỨC

21st May 2010, Chicago, Illinois

iTWeb

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 bất 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 hơn và trả tiền thường xuyên hơn để người dùng tin

Đánh 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
- Cạnh 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

FOOTPRINTING

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

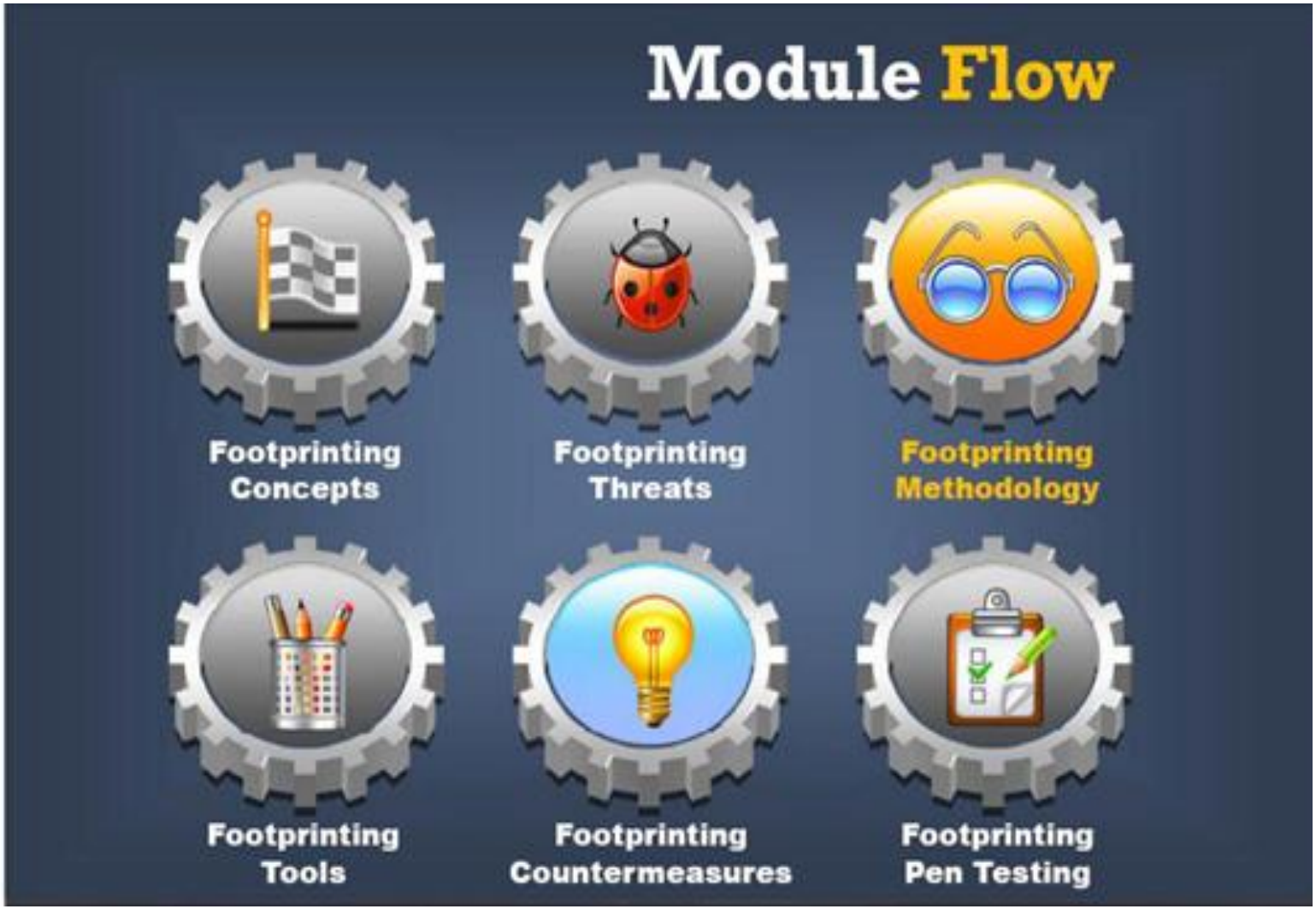
Objectives of Footprinting

 thu thập thông tin mạng	• Tên domain • Tên domain nội bộ • Khối kết nối mạng • Dia chi ip cua thể truy cập hệ thống • Giả mạo web/ cá nhân web • Máy chủ chạy TCP và UDP •	• Giao thức mạng • Quan điểm VPN • ACLs • chạy IDSes • tín hiệu tương tự/ tín hiệu số điện thoại • xác thực các cơ chế •
 thu thập thông tin hệ thống	• Người dùng và tên nhóm • Hệ thống biểu ngữ • Bảng định tuyến • Thông tin SNMP	• Mô hình hệ thống • Kiểu hệ thống từ xa • Tên hệ thống • Mật khẩu
 Thu thập thông tin về tổ chức	• Thông tin nhân viên • Tổ chức web • Danh sách công ty	• Địa chỉ và sdt • Nền tảng về tổ chức • Tin tức về các bài viết/ phát hành các bài báo

FOOTPRINTING

FOOTPRINTING

FOOTPRINTING

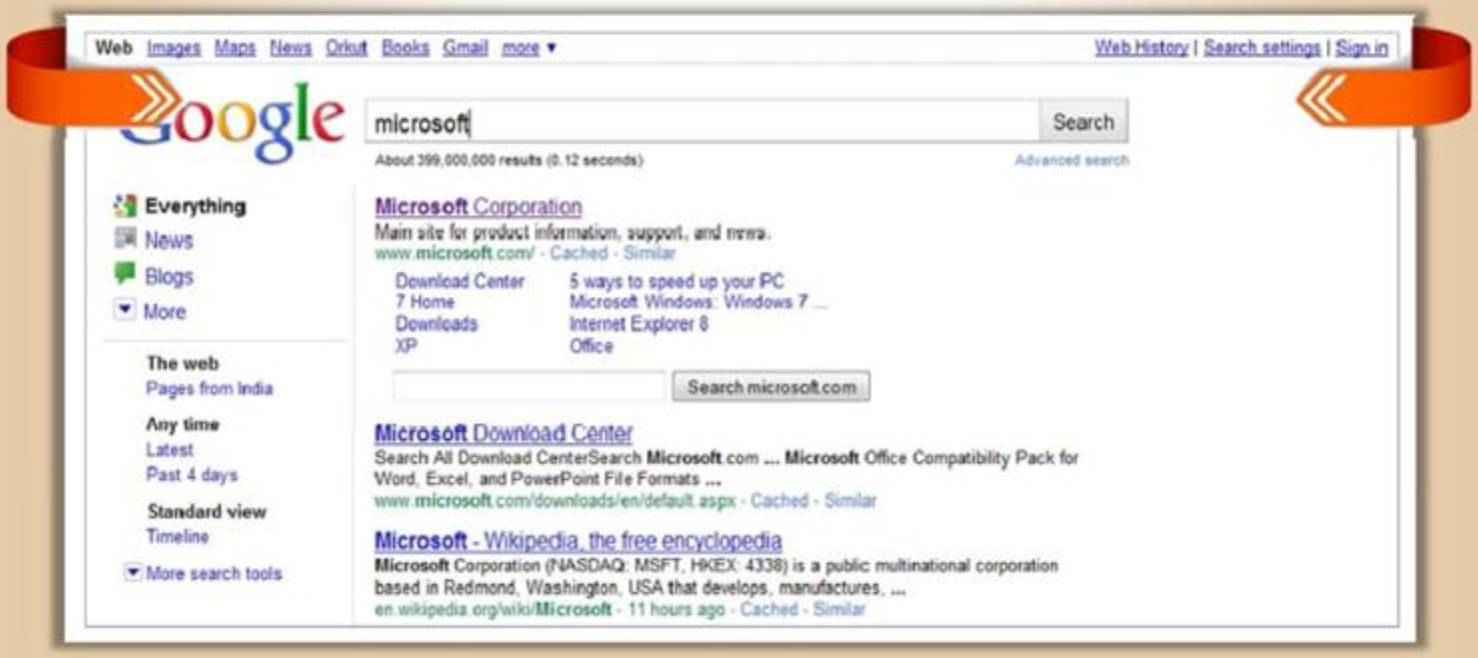


FOOTPRINTING

FOOTPRINTING

Tìm kiếm một công ty thông qua URL

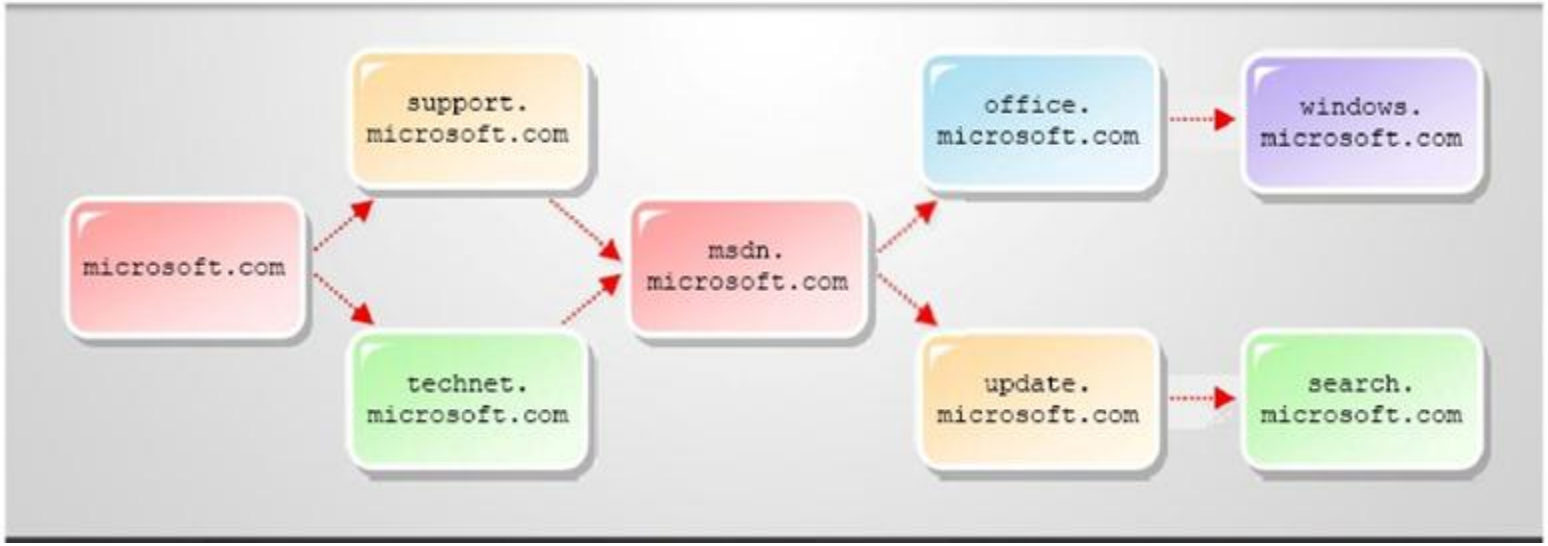
- Tìm kiếm các công ty mục tiêu với một số công cụ tìm kiếm như Google hoặc Bing



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

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 intenet 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 chẳng hạn như nền tảng công nghệ, chi tiết nhân viên, các trang đăng nhập, mạng nội bộ cổng thông tin, giúp thực hiện kỹ thuậtvà 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).

FOOTPRINTING

Thu thập vị trí thông tin

Google

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

http://earth.google.com

FOOTPRINTING

Hình ảnh vệ tinh của một nơi cư trú

FOOTPRINTING

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

FOOTPRINTING

Mọi người tìm kiếm máy chủ trực tuyến

http://www.intelius.com

http://www.bestpeoplesearch.com

http://people-search-america.com

http://www.anywho.com

FOOTPRINTING

Mọi người tìm kiếm các dịch vụ trực tuyến

Yahoo People Search
http://people.yahoo.com

Address.com
http://www.address.com

123 People Search
http://www.123people.com

Zaba Search
http://www.zabasearch.com

Wink People Search
http://wink.com

Public People Finder
http://www.publicpeoplefinder.com

People Finders
http://www.peoplefinders.com

People Lookup
https://www.peoplelookup.com

FOOTPRINTING

Mọi người tìm kiếm trên dịch vụ mạng xã hội

FOOTPRINTING

Thu thập thông tin từ các dịch vụ tài chính

Google Finance

Yahoo Finance

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
17123.6554670.6
42319173004

Location
Boca Raton, FL 33487

Job Status
IT/Software Development

Apply Now

Become a Fan on facebook.

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
- Bachelorâ€™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 canh tranh hoặc các ngành công nghiệp

FOOTPRINTING

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

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

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

ChoicePoint Online
http://www.choicepointonline.com

Tiền bỏ ra cho các
công ty nghiên cứu
http://money.cnn.com

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

Forbes 500
http://www.forbes.com

Barrons
http://online.barrons.com

FOOTPRINTING

Các công ty tư vấn cạnh tranh thông minh

http://www.carratu.com

http://www.fuld.com

http://www.globalintelligence.com

http://www.datamonitor.com

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.iptools.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(pham vi)

vùng mạng Internet đăng ký

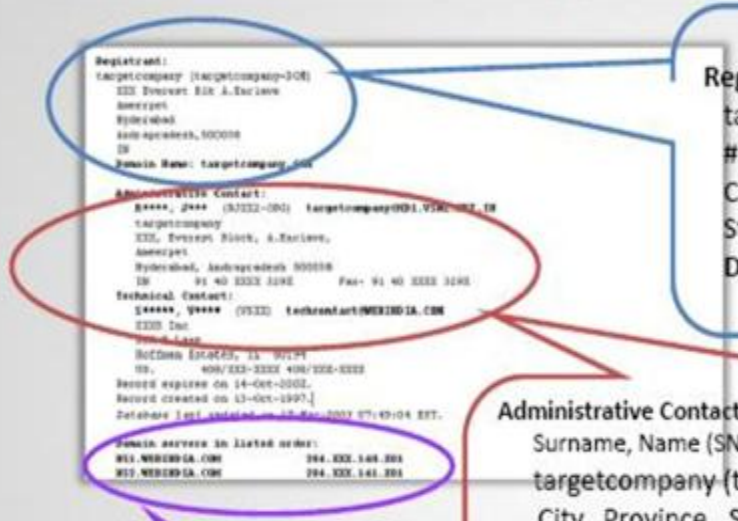
1. AfriNIC
2. ARIN
3. APNIC
4. LACNIC, RIPE NCC

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)
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

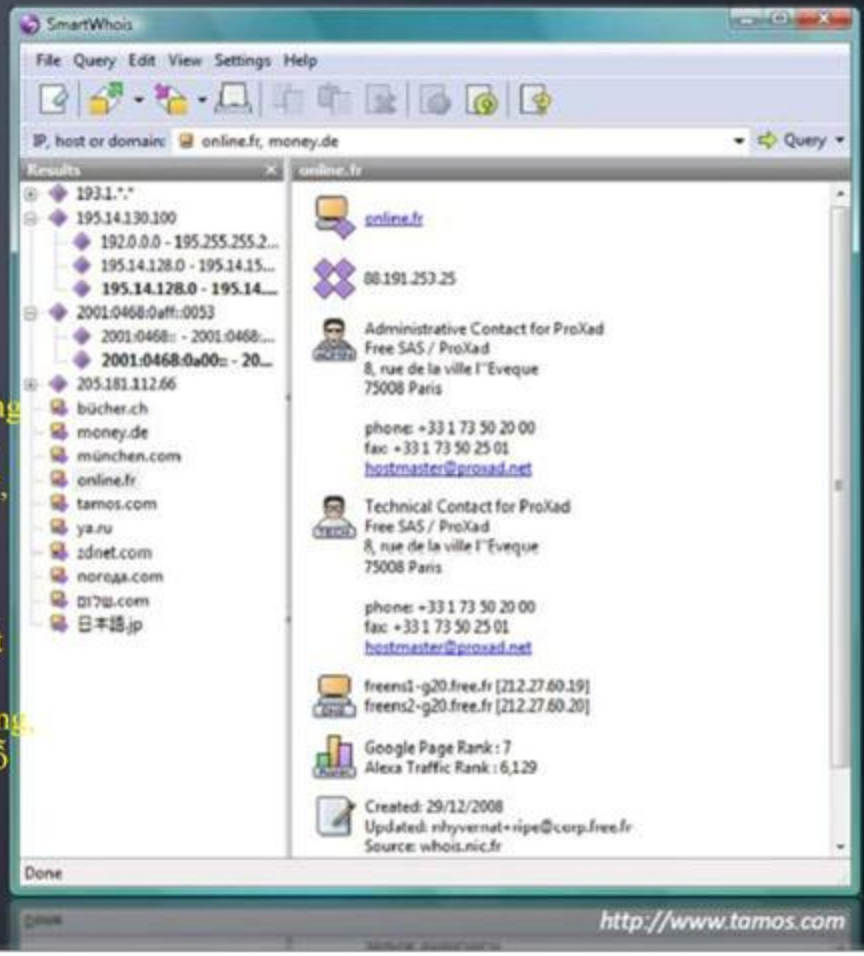
Domain servers in listed order:
NS1.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

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

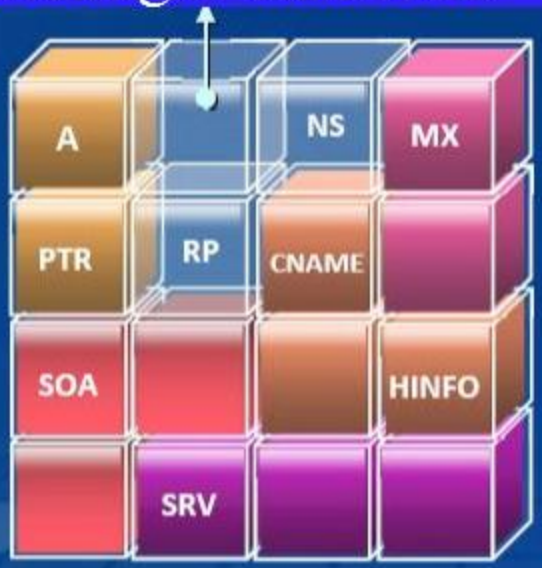
- **Whois** — http://tools.whois.net
- **Whois Lookup** — http://www.iptools.com
- **Better Whois** — http://www.betterwhois.com
- **Geek Whois** — http://www.geektools.com
- **Arin Whois Database Search** — http://whois.arin.net
- **Network Solutions Whois** — http://www.networksolutions.com
- **DomainTools** — http://www.domaintools.com
- **AutoWhois** — http://centralops.net

FOOTPRINTING

FOOTPRINTING

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

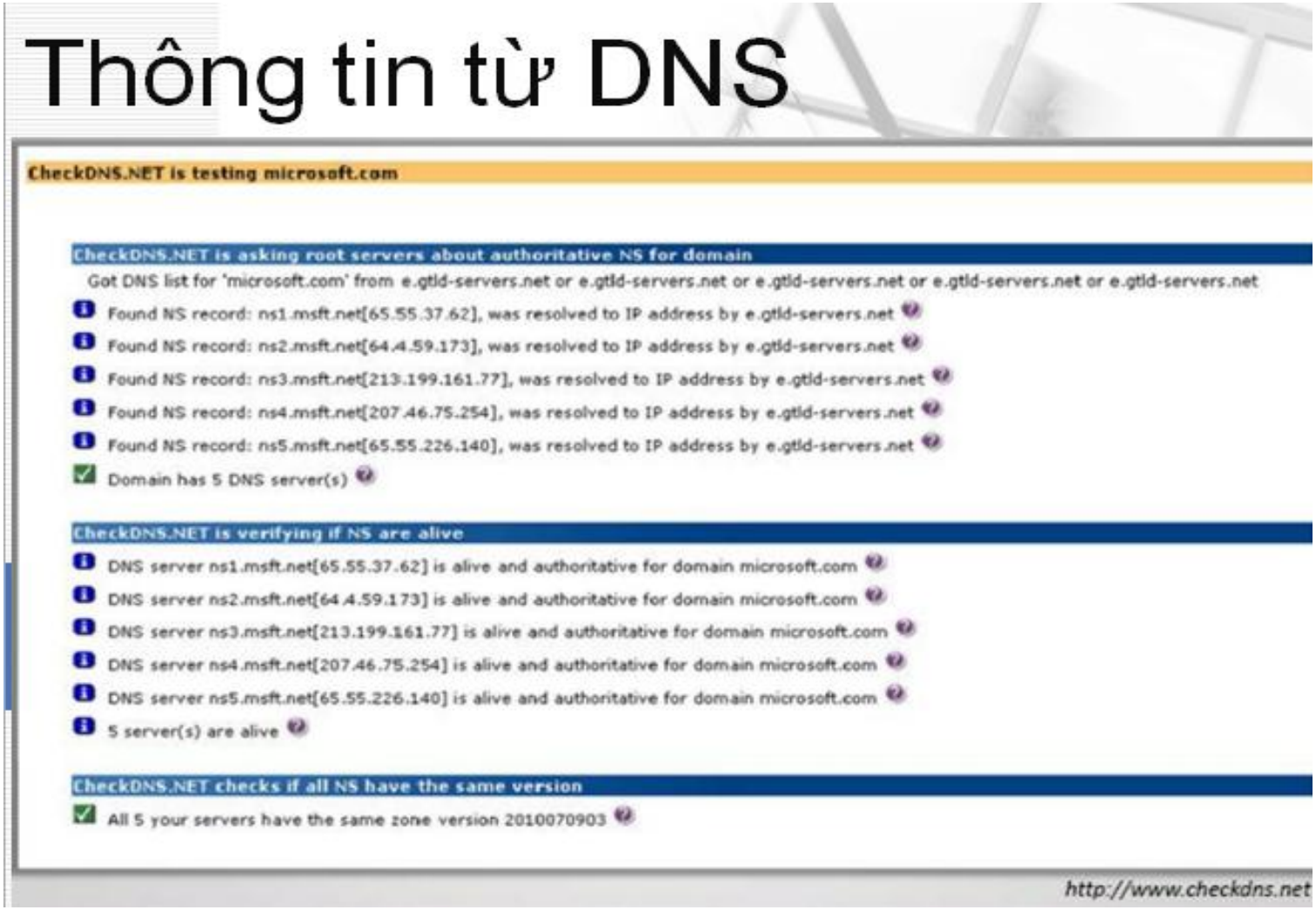
- **A** - Trỏ đến một địa chỉ ip host
- **MX** - Trỏ đến tên miền của máy chủ mail
- **NS** - Trỏ đến tên miền của máy chủ
- **CNAME** - Quy tắc đặt tên cho một máy chủ
- **SOA** - Cho biết ý nghĩa của một tên miền
- **SRV** - Thông tin của một dịch vụ
- **PTR** - Giả mạo địa chỉ ip của một máy chủ
- **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://network-tools.com
- http://www.checkdns.net
- http://www.iptools.com

FOOTPRINTING

Thông tin từ DNS



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

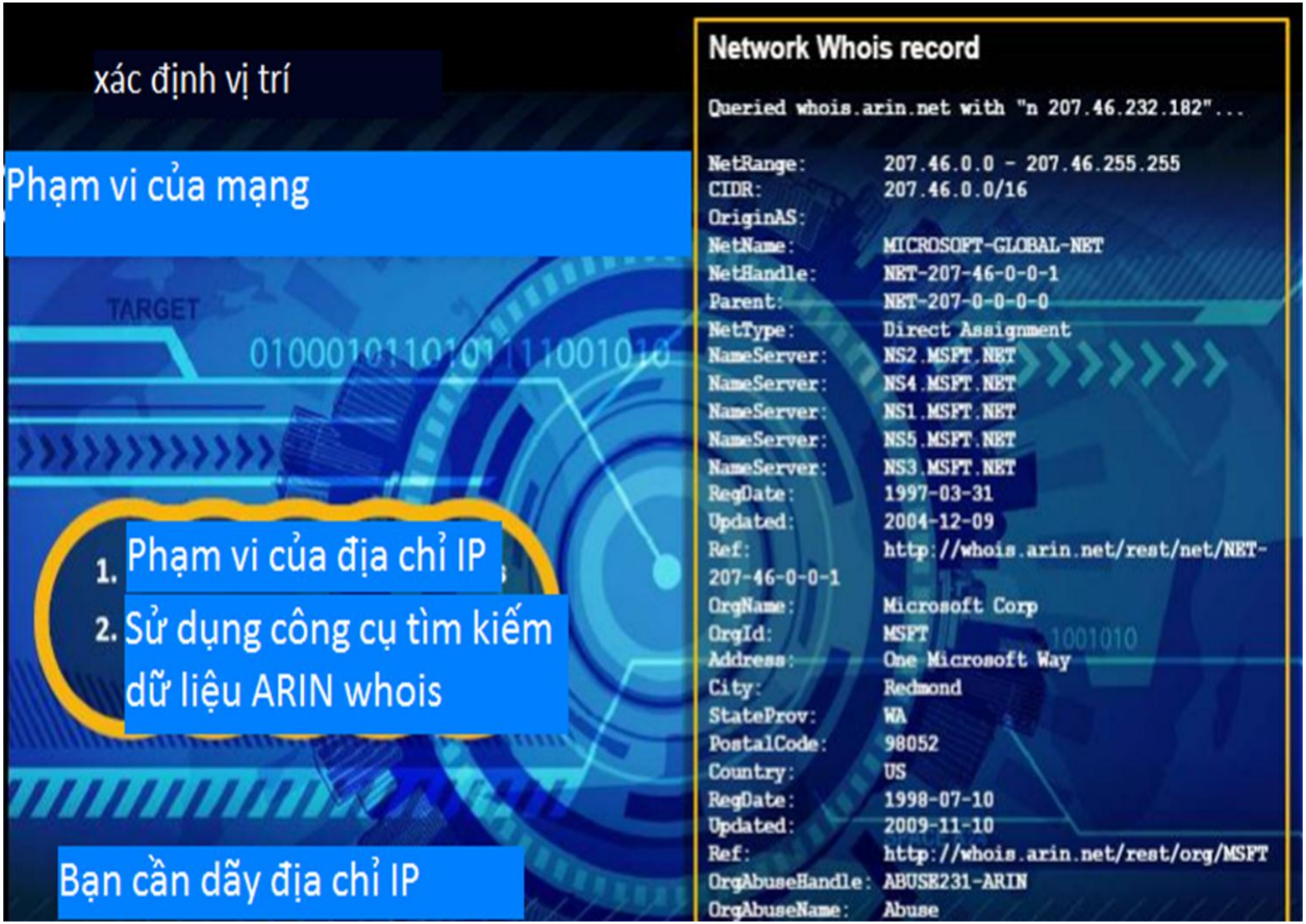
Mozzle Domain Name Pro
http://www.mozzle.com

Check DNS
http://www.checkdns.net

Domain Information Groper
http://www.kloth.net

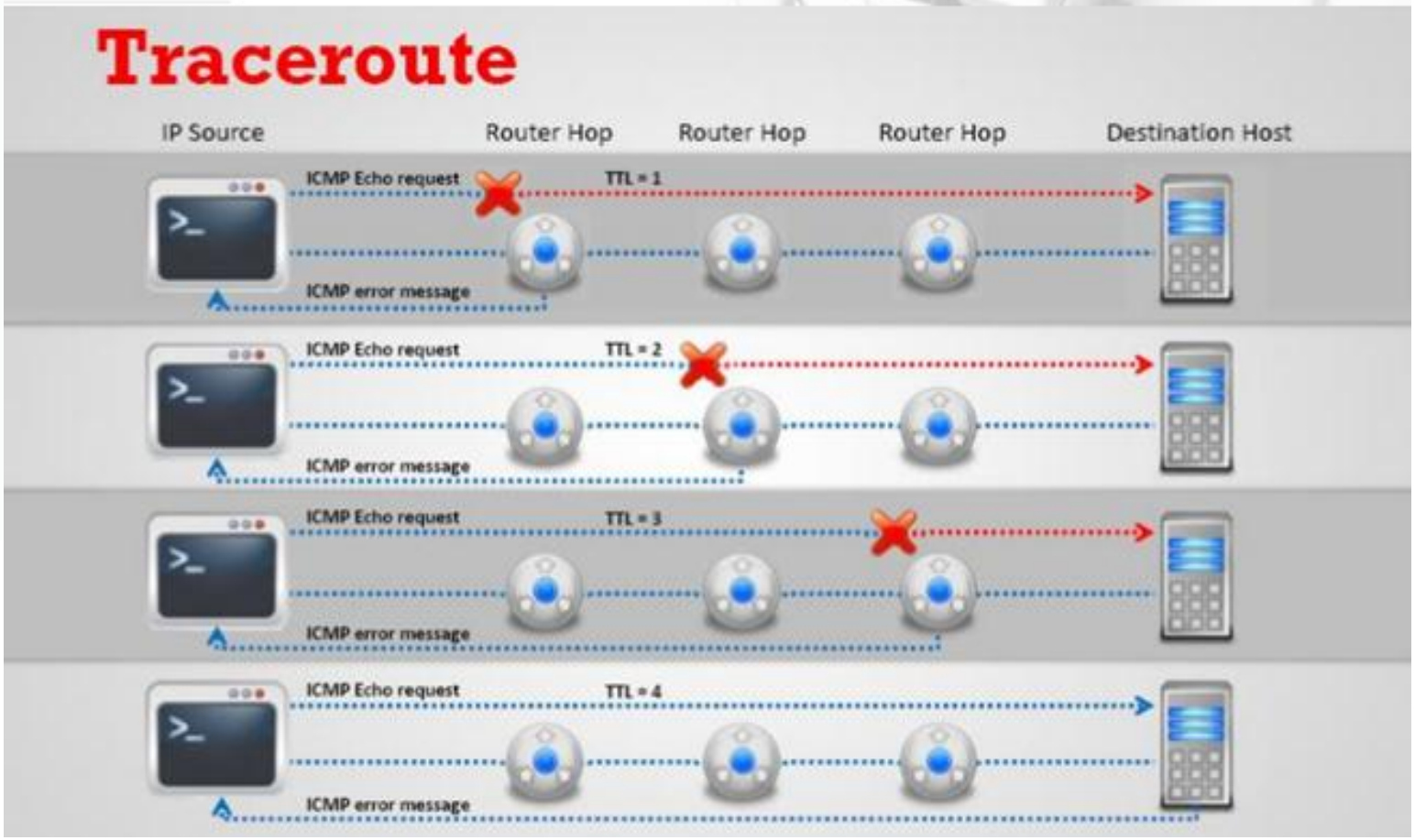
FOOTPRINTING

FOOTPRINTING



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.



FOOTPRINTING

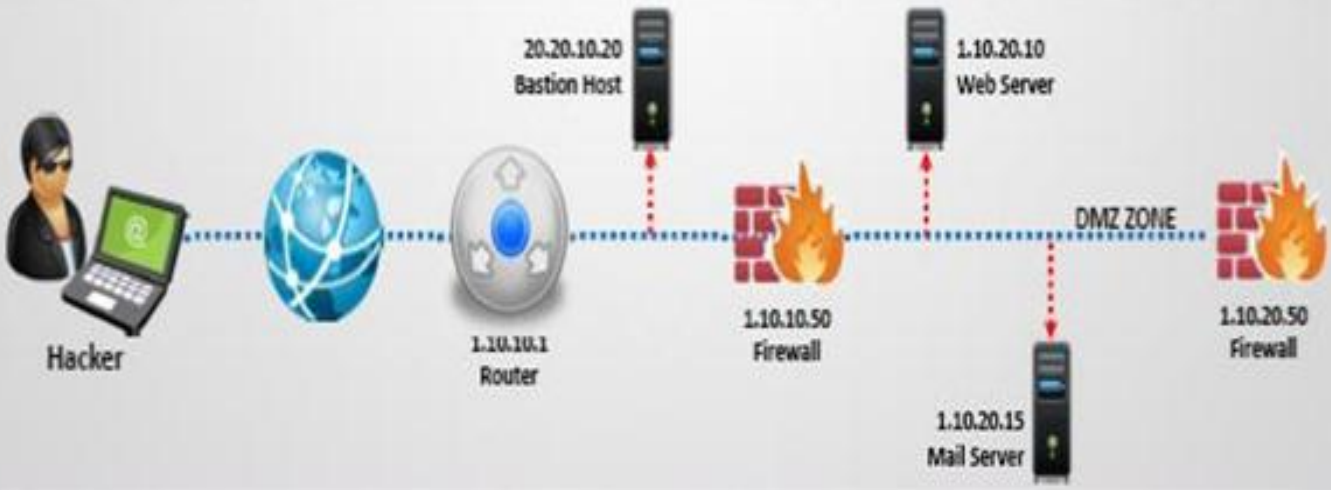
Phân tích chương trình Traceroute

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:

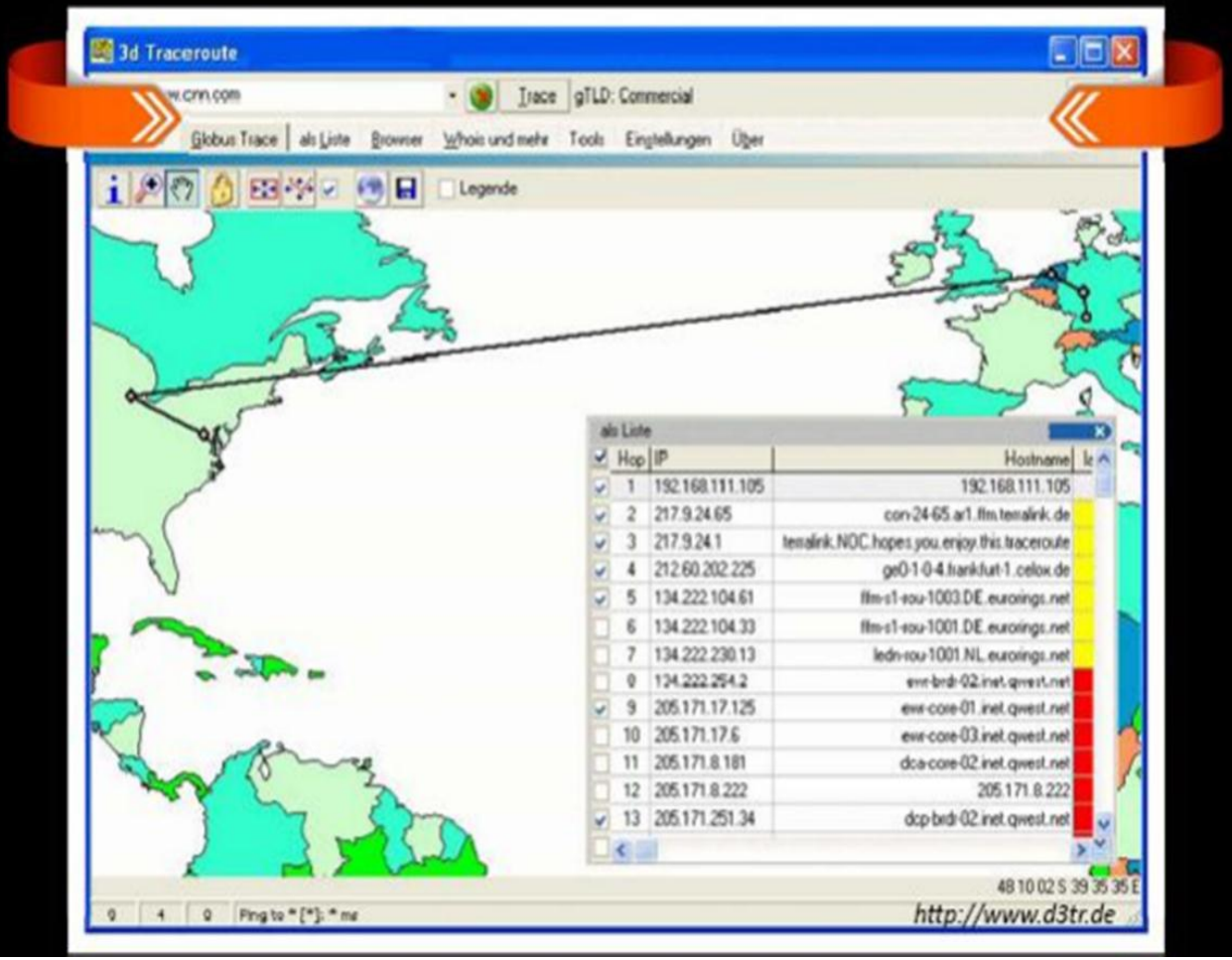
- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1z
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

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



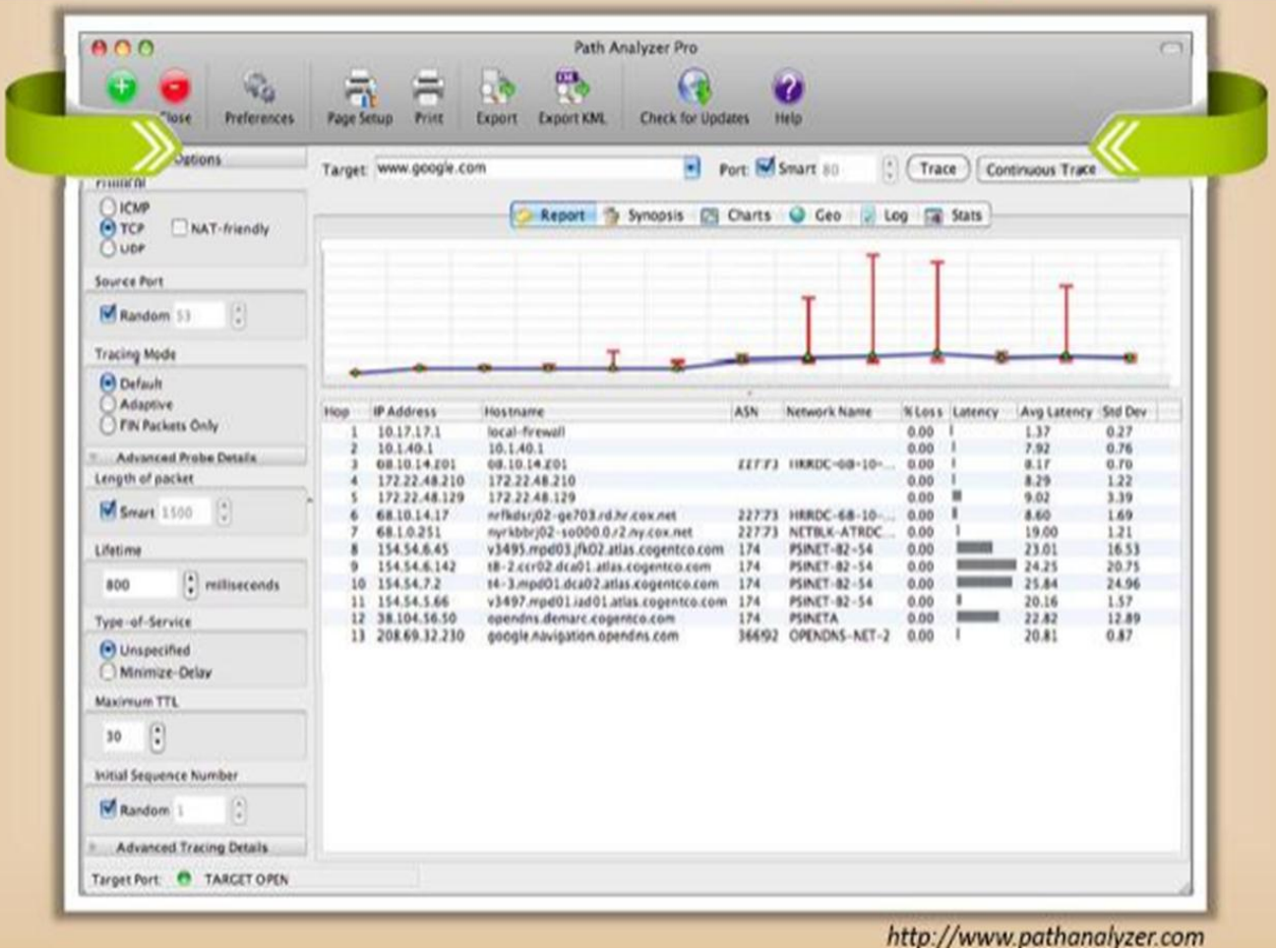
FOOTPRINTING

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

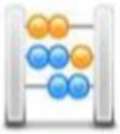
Tcp Trace Route
http://michael.toren.net

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

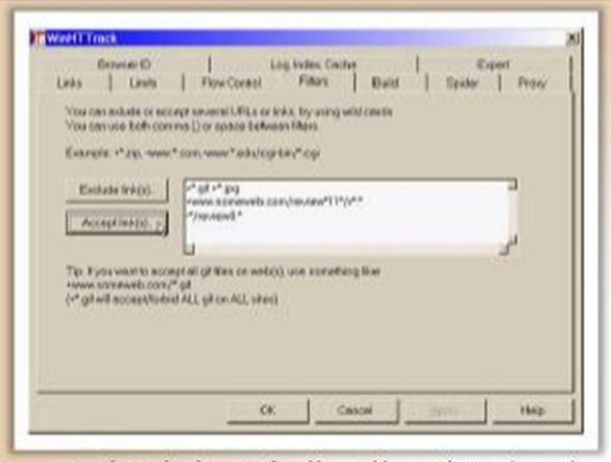
FOOTPRINTING

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

FOOTPRINTING

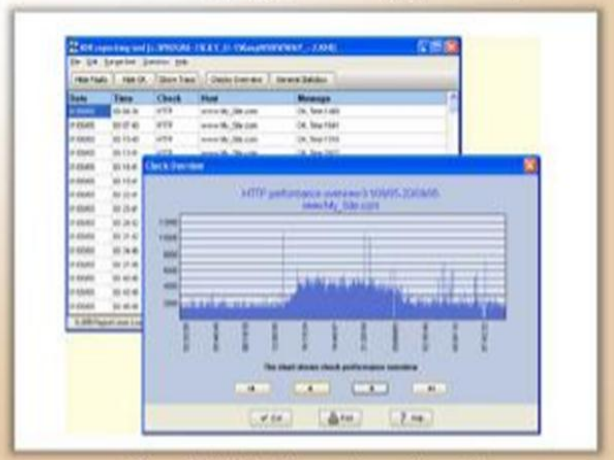
Công cụ là trang web của Mirroring



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

WinWSD
http://winwsd.uw.hu

Reamweaver
http://reamweaver.com

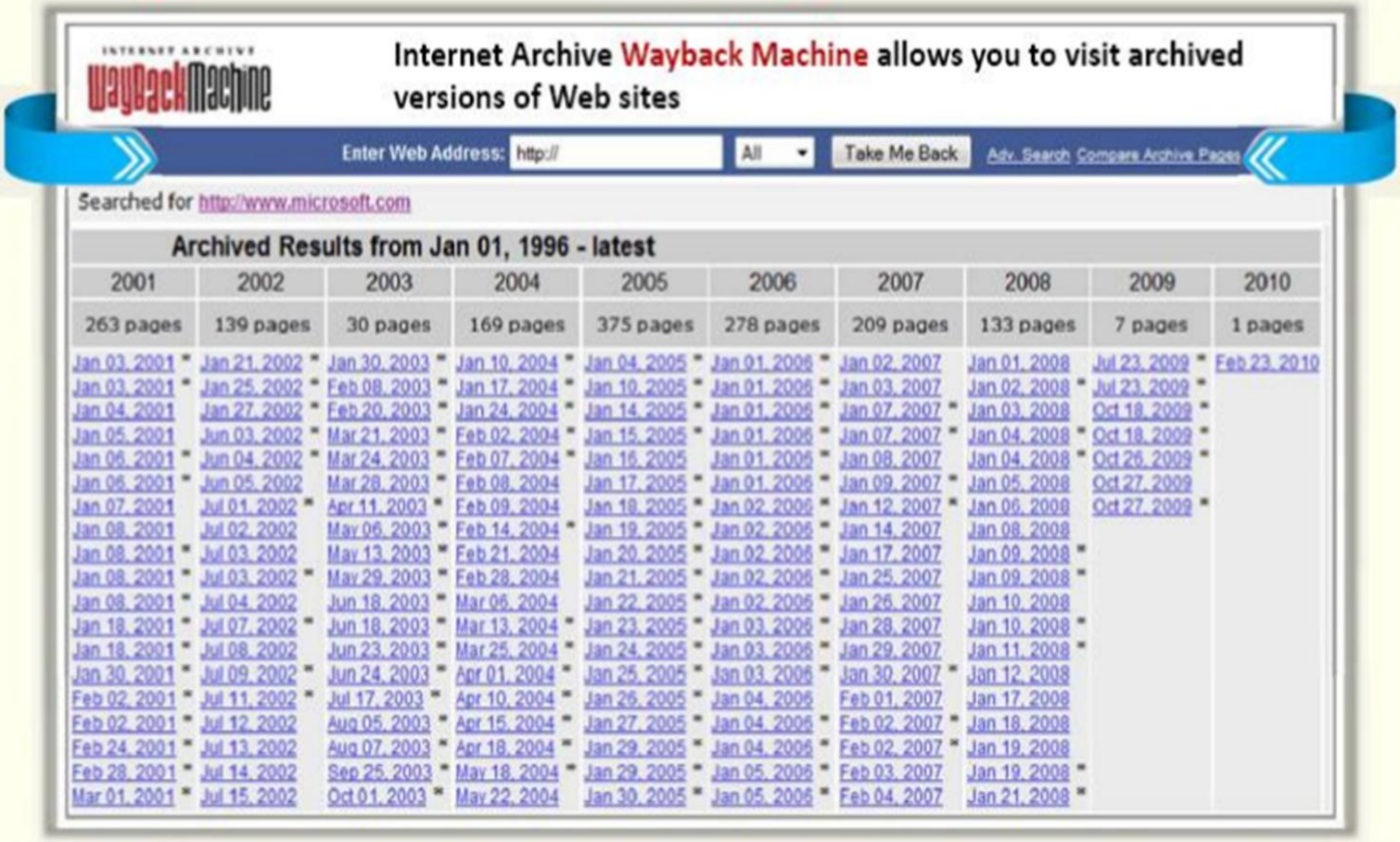
xaldon webspider 2
http://www.xaldon.de

Teleport Pro
http://www.tenmax.com

FOOTPRINTING

VD: Bảng thông tin của trang web

http://www.archive.org



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

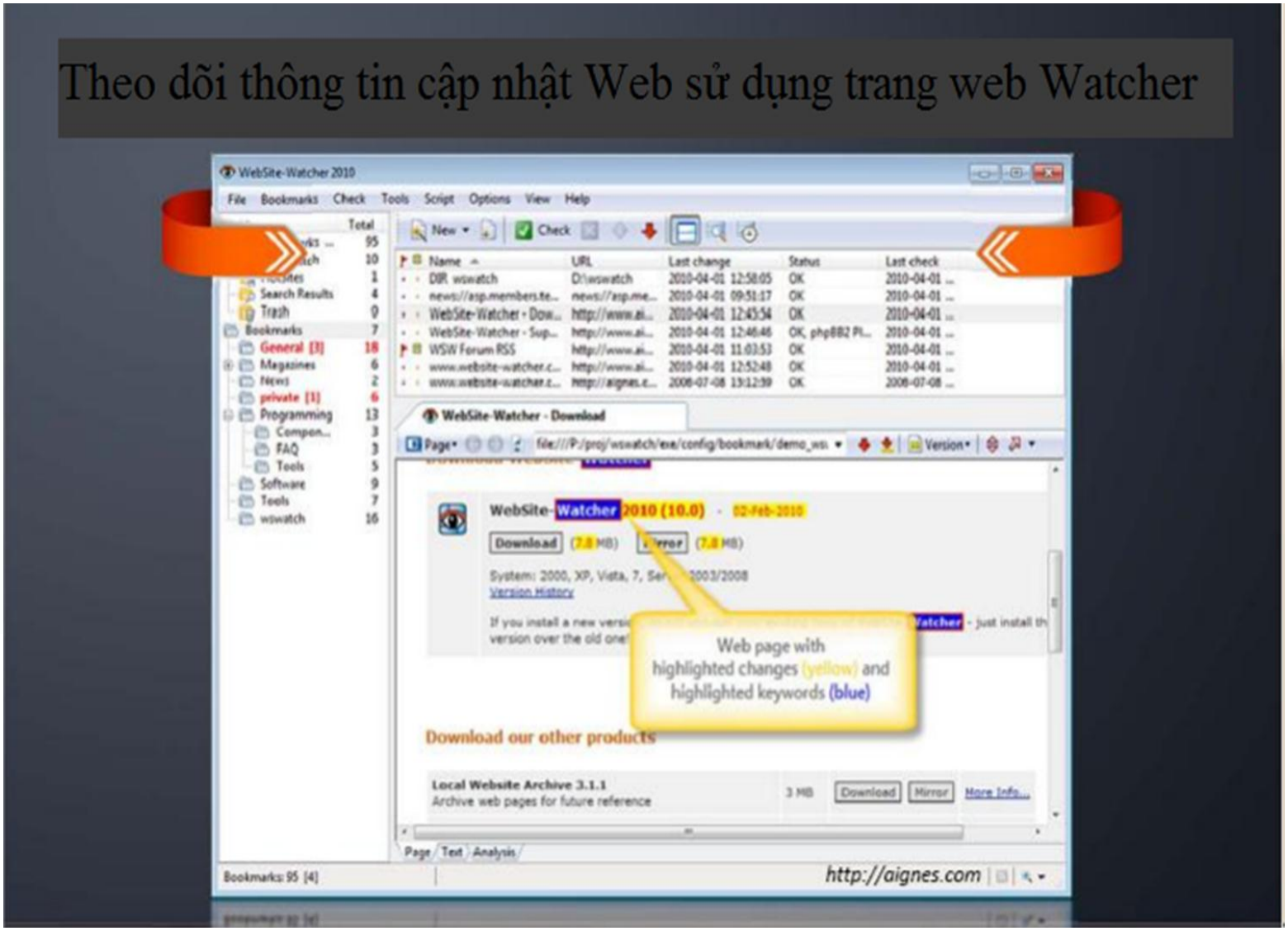
Enter Web Address: http:// | All | Take Me Back | Adv. Search | Compare Archive Pages

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



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

FOOTPRINTING

Email Tracking Tools

eMailTrackerPro
http://www.emailtrackerpro.com

Read Notify
http://www.readnotify.com

DidTheyReadIt
http://www.didtheyreadit.com

PoliteMail
http://www.politemail.com

FOOTPRINTING

Email là công cụ theo dõi

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

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 nhhà điều hành

Nó sử dụng google để khai thác xác định vị trí của các chủi cụ thể

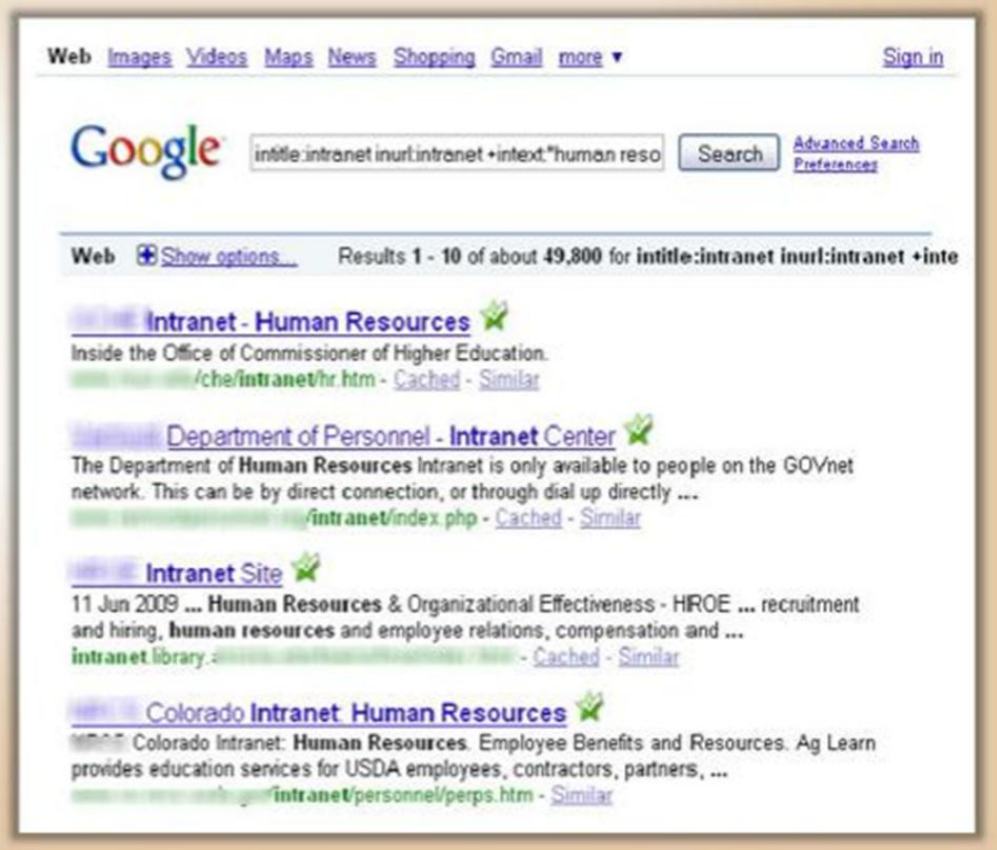
FOOTPRINTING

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



FOOTPRINTING

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

FOOTPRINTING

Công cụ hacking Google

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

Google Cartography
http://richard.jones.name

Goolink Scanner
http://www.ghacks.net

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

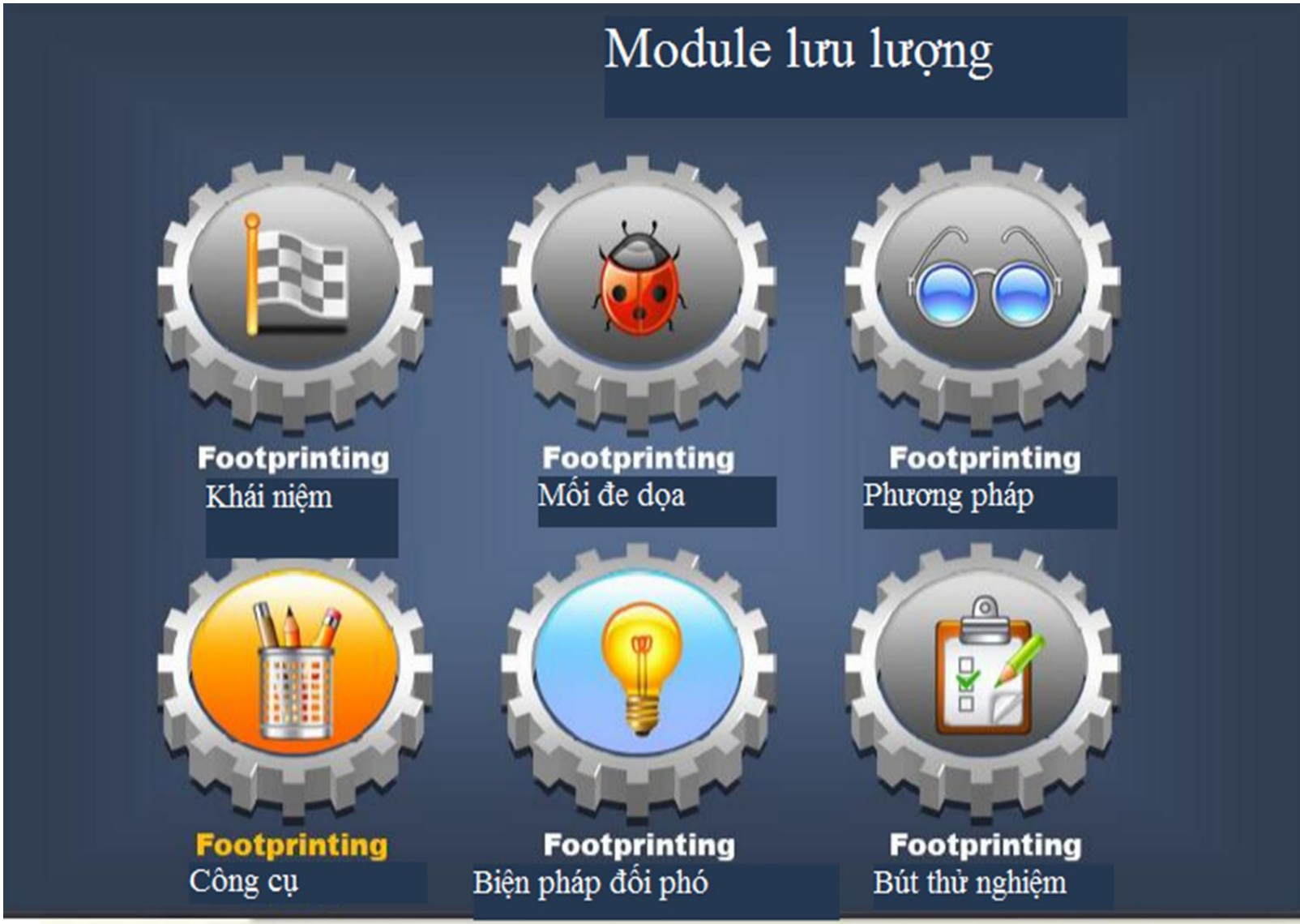
SiteDigger
http://www.foundstone.com

GMapCatcher
http://code.google.com

Google Hacks
http://code.google.com

BiLE Suite
http://www.sensepost.com

FOOTPRINTING



FOOTPRINTING

Các công cụ Footprinting

Prefix WhoIs
http://pwhois.org

DMitry (Deepmagic Information Gathering Tool)
http://www.mor-pah.net

Tctrace
http://www.phenoelit-us.org

Autonomous System Scanner(ASS)
http://www.phenoelit-us.org

NetScanTools Pro
http://www.netscantools.com

Netmask
http://www.phenoelit-us.org

Maltego
http://www.paterva.com

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.mozdev.org

DomainInspect
http://www.antssoft.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

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 hoá các danh sách thư mục và sử dụng split-DNS

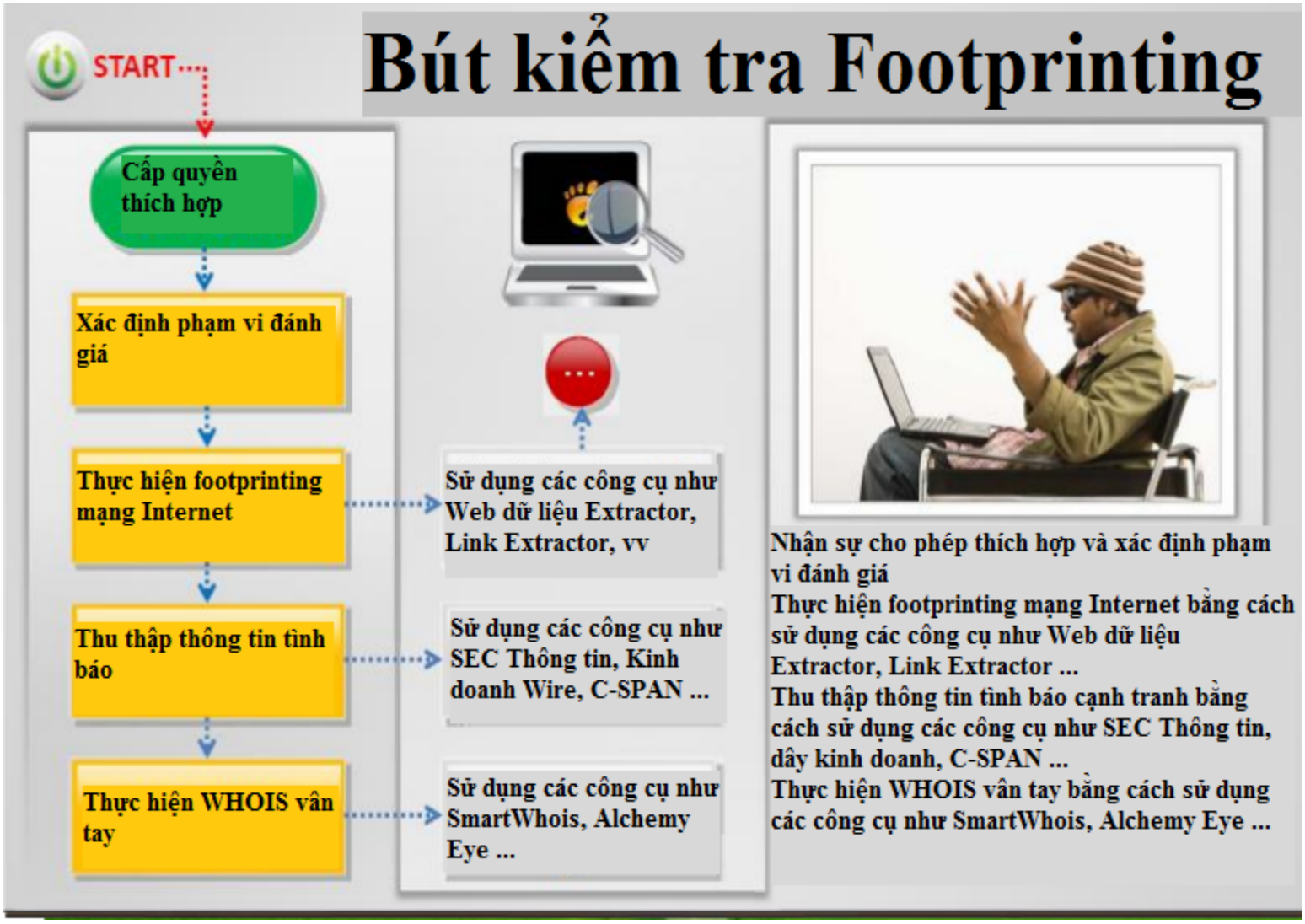
FOOTPRINTING

Bút kiểm tra Footprinting

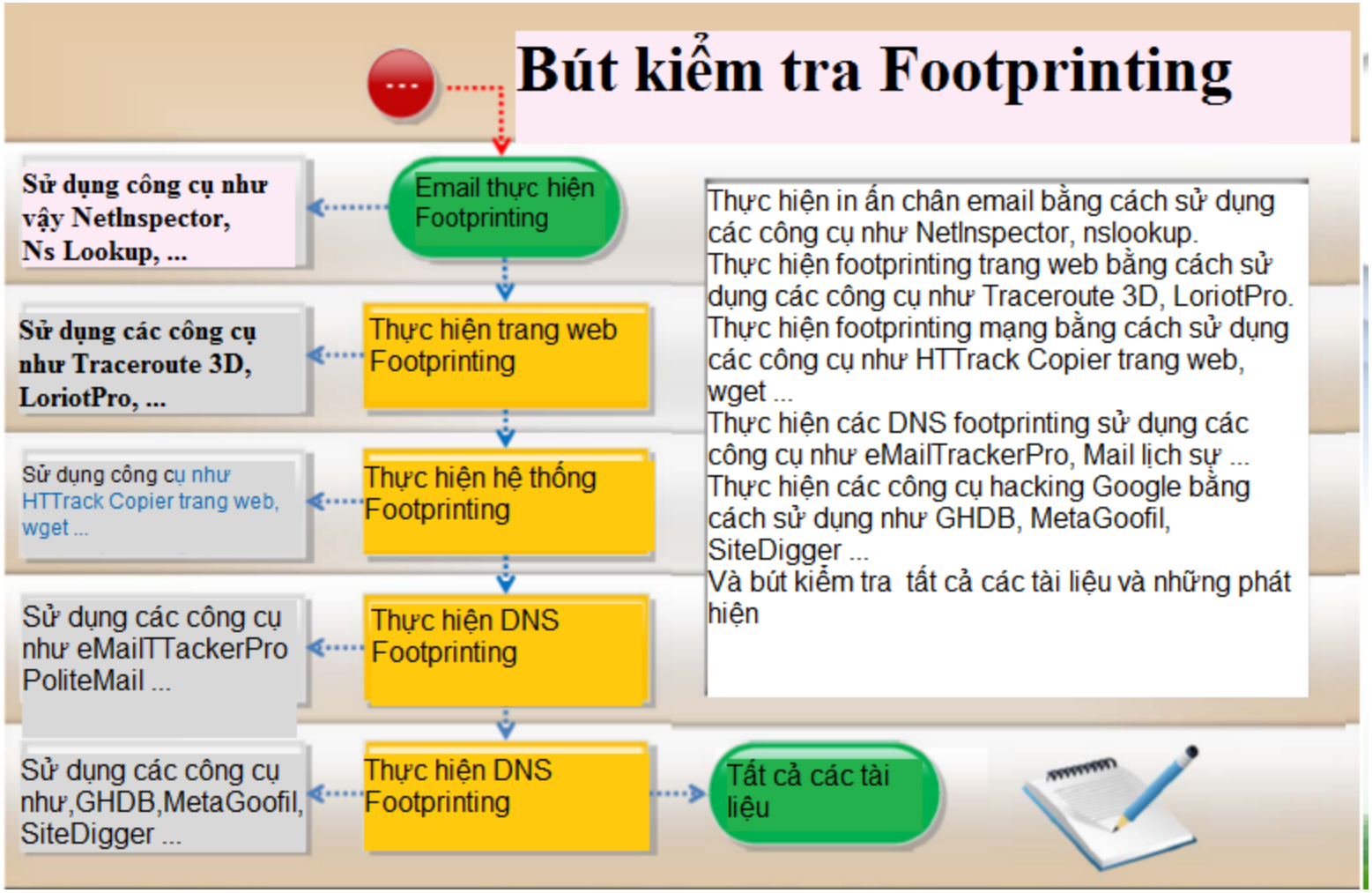
+ Bút Footprinting được sử dụng để kiểm tra và xác định thông tin của tổ chức công bố công khai trên Internet như kiến trúc mạng, hệ điều hành, ứng dụng và người sử dụng
+ Kiểm tra để thu thập càng nhiều thông tin càng tốt về tổ chức mục tiêu từ internet và các nguồn truy cập công cộng khác

FOOTPRINTING

Bút kiểm tra Footprinting



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

FOOTPRINTING

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