Footprinting and Reconnaissance

Module 2

Engineered by **Hackers**. Presented by Professionals.

CEH
Certified Ethical Hacker

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

SECURITY NEWS

iWeb

21st May 2010, Chicago, Illinois

Battle Against Data Theft

There is a general misconception that cyber-criminals select only high worth users and the majority of Internet users underestimate the risk of illegal access to their data.

In a recent survey conducted by Avira, 10% of Internet users confirmed they had been victims of some form of data theft, of whom 4% had suffered actual financial loss and the remaining 6% had been victims of identity theft.

As cyber-criminals become more ingenious, detection of unusual behavior or reduced system performance is now only possible with extensive security protection.

Greater sophistication of potentially unwanted applications (PUAs) means their presence remains undetected for longer and small pay-offs are far more frequent that users believe.

Data theft from e-mail and online accounts (Facebook and eBay) or careless responses to online scams may be all that is required.

http://www.itweb.co.za

Certified Ethical Hacker

Professional Training Services

CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Module Objectives

- What is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Internet Footprinting
- Competitive Intelligence
- WHOIS Footprinting
- DNS Footprinting

- Network Footprinting
- Website Footprinting
- E-mail Footprinting
- Google Hacking
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing

3

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting Terminologies

Open Source or Passive Information Gathering

Collect information about a target from the publicly accessible sources

Active Information Gathering

Gather information through social engineering on-site visits, interviews, and questionnaires

Anonymous Footprinting

Gather information from sources where the author of the information cannot be identified or traced

Pseudonymous Footprinting

Collect information that might be published under a different name in an attempt to preserve privacy

Organizational or Private Footprinting

Collect information from an organization's web-based calendar and email services

Internet Footprinting

Collect information about a target from the Internet

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

http://ceh.vn

Objectives of Footprinting

Collect Network Information

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- Networking protocols
- VPN Points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms

Collect System Information

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords

Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Address and phone numbers
- Background on the organization
- News articles/press releases

http://ceh.vn

EH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting **Threats**

- Attackers gathers valuable **system-level information** such as account details, operating system and other software versions, server names, and database schema details from footprinting techniques

Threats include:

- Business loss
- Corporate espionage
- Privacy loss
- Social engineering
- System and network attacks
- Information leakage

9

CEH
Certified Ethical Hacker

Finding a Company's URL

Search for the target company in a search engine such as **Google** or **Bing**

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Locate Internal URLs

- Internal URLs **provide an insight** into different departments and business units in an organization
- You may find an internal company's URL **by trial and error method**
- **Tools** to search internal URLs:
  - *http://news.netcraft.com*
  - *http://www.webmaster-a.com/link-extractor-internal.php*

microsoft.com → support.microsoft.com

microsoft.com → technet.microsoft.com

support.microsoft.com → msdn.microsoft.com

technet.microsoft.com → msdn.microsoft.com

msdn.microsoft.com → office.microsoft.com

office.microsoft.com → windows.microsoft.com

msdn.microsoft.com → update.microsoft.com

update.microsoft.com → search.microsoft.com

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Public and Restricted Websites

■ Identify a company's private and public websites

Public website
http://www.apple.com

Restricted website
http://developer.apple.com

CEH
Certified Ethical Hacker

14

Search for Company's Information

Search
1. Search for a company's information in major search engines, such as Google or Bing
2. Use complex keywords to search about a company

Information
1. Updates made to the website
2. Employee database
3. Press releases
4. Contact information

Techniques
1. Extract archive and mirror website
2. Search the web
3. People search
4. Competitive intelligence

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Tools to Extract Company's Data

I Web Data Extractor (*http://www.webextractor.com*)

- Web Data Extractor **extracts the targeted company's contact data** (email, phone, fax) from the Internet

II SpiderFoot (*http://www.binarypool.com*)

- SpiderFoot is a domain footprinting tool which will **scrape the websites** on that domain, as well as search Google, Netcraft, Whois, and DNS to collect the company information

III Robtex (*http://www.robtex.com*)

- Robtex utilites **crawl the Internet** using the useragent "robtexbot," mainly to get title and meta information

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
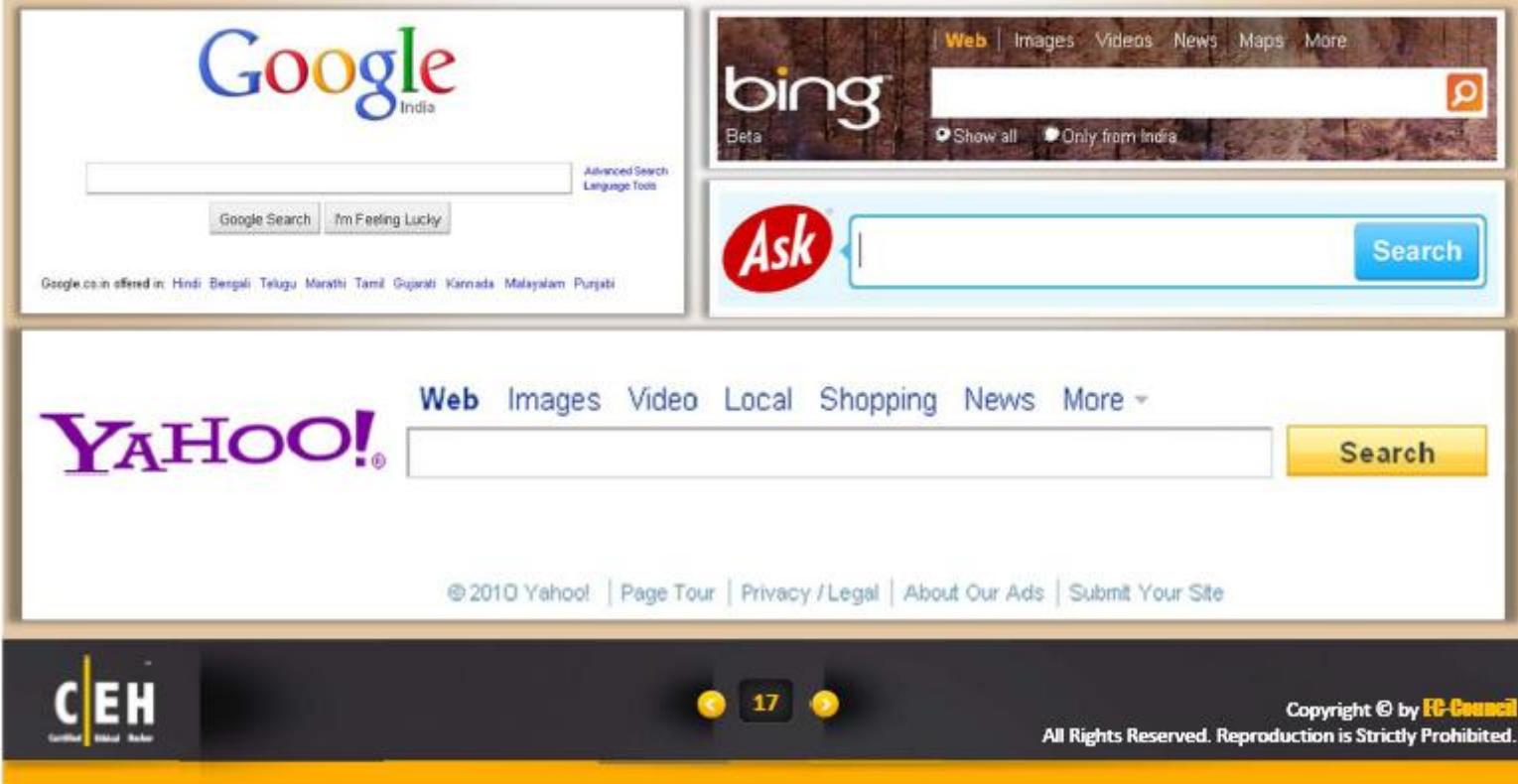
# Footprinting Through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks

- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)
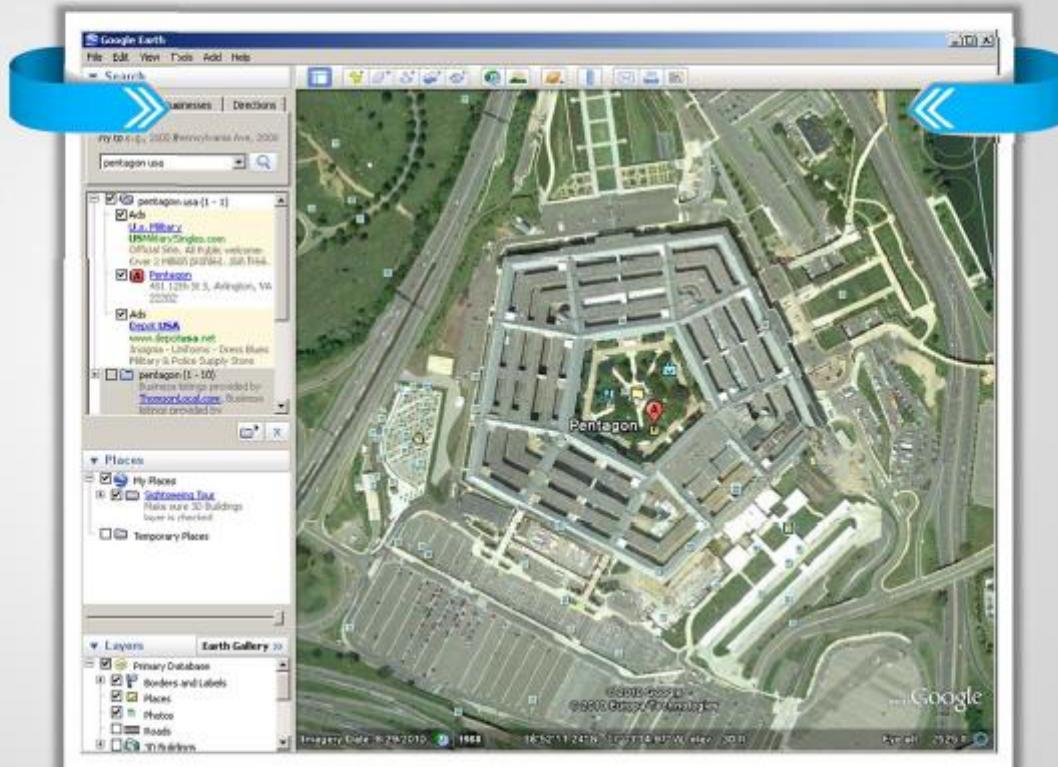
Collect Location Information

Use **GoogleEarth** tool to get the location of the place

http://earth.google.com

http://ceh.vn
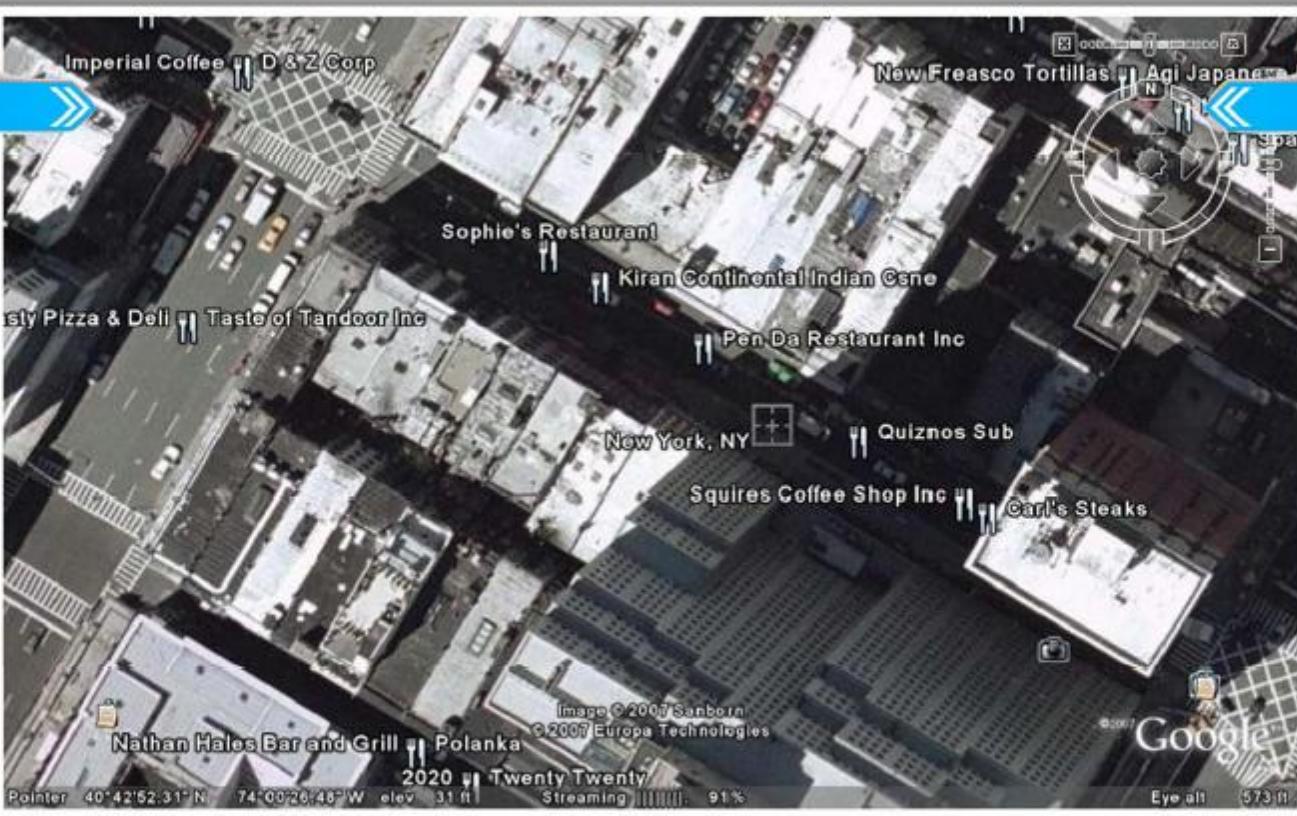
http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Satellite Picture of a Residence

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

People Search

The people search returns the following information about a person:

- Residential addresses
- Contact numbers
- Date of birth
- E-mail addresses
- Satellite pictures of the private residences

Premium Public Records (24)

ALL | INTELIUS | US SEARCH | peoplefinders

peoplesmart

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

Bill J Clinton (age: 64)
61571 WASHINGTON, IL - view details

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

100 entries for Bil 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

Address: 15050 NE 99th Way Bellevue, WA 98004

Phone Number: (425) 555-XXXX

Aliases: 1) Lorry Ortiz 2) Samatha Ortiz

Age: 37

You can find **personal information** using online people search services

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

People Search Using http://pipl.com

- Pipl uses a technique known as **"the deep web"** to extract information about people

- The term **"deep web"** refers to a vast repository of underlying content, such as documents in online databases that general-purpose **web crawlers** cannot reach

pipl

The most comprehensive people search on the web

Name Email Username Phone   BETA Business

| First Name | Last Name | City | State | Country |

Search   Clear

What's so different about pipl?

Terms Privacy Directory Contact
©2006-2010 Pipl

21

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

People Search Online Services

http://www.intelius.com

http://www.bestpeoplesearch.com

http://people-search-america.com

http://www.anywho.com

People Search Online Services

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

http://ceh.vn

EH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

People Search on Social Networking Services

http://www.orkut.com

http://www.facebook.com

http://www.linkedin.com

http://twitter.com

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting Through Job Sites

You can gather a **company's infrastructure details** from job postings

Look for these information:

➤ Job requirements

➤ Employee's profile

➤ Hardware information

➤ Software information

Job ID
17123.6554670.6
42319173004

Location
Boca Raton, FL 33487

Job Status
IT/Software Development

▶ Apply Now

f 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

CEH

26

Monitoring Target Using Alerts

- Google Alerts is a content monitoring service that automatically **notifies users** when new content from news, web, blogs, video and/or discussion groups matches a set of search terms selected by the user and stored by the Google Alerts service

- Google Alerts help in **monitoring** a developing news story and keeping current on a competitor or industry

GigaAlert — Generate Leads. Monitor Competitors. Safeguard Your Reputation.

Track your interests on the Web.

Sign Up ▶   Log In ▶

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

© 2010 Indigo Stream Technologies, provider of Copyscape. Giga Alert was formerly known as Google Alert. Terms of use.

Login   About   Products   Testimonials   Press

Google alerts beta

Search terms:	Preview results
Type:	Everything
How often:	once a day
Email length:	up to 20 results
Your email:	

Create Alert

CEH
Certified Ethical Hacker

◀ 27 ▶

EH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Competitive Intelligence Gathering

"Business moves fast. Product cycles are measured in months, not years. **Partners become rivals quicker than you can say "breach of contract."** So how can you possibly hope to keep up with your competitors if you can't keep an eye on them?"

The competitive intelligence is **non-interfering and subtle in nature**

Competitive intelligence is the process of **identifying, gathering, analyzing, verifying, and using information** about your competitors from resources such as the Internet

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Competitive Intelligence Gathering

1. Compare your products with your competitors' offerings

2. Analyze your market positioning compared to the competitors

3. Pull up a list of competing companies in the market

4. Extract salespersons' war stories on how deals are won and lost in the competitive arena

5. Produce a profile of the CEO and the entire management staff of the competitor

30

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

When did it begin?

When
How

Where is it located?

Company

How did it develop?

Where
Who

Who leads it?

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

CEH

31

http://ceh.vn

CEH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Competitive Intelligence - What are the Company's Plans?

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*)

CEH
Certified Ethical Hacker

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
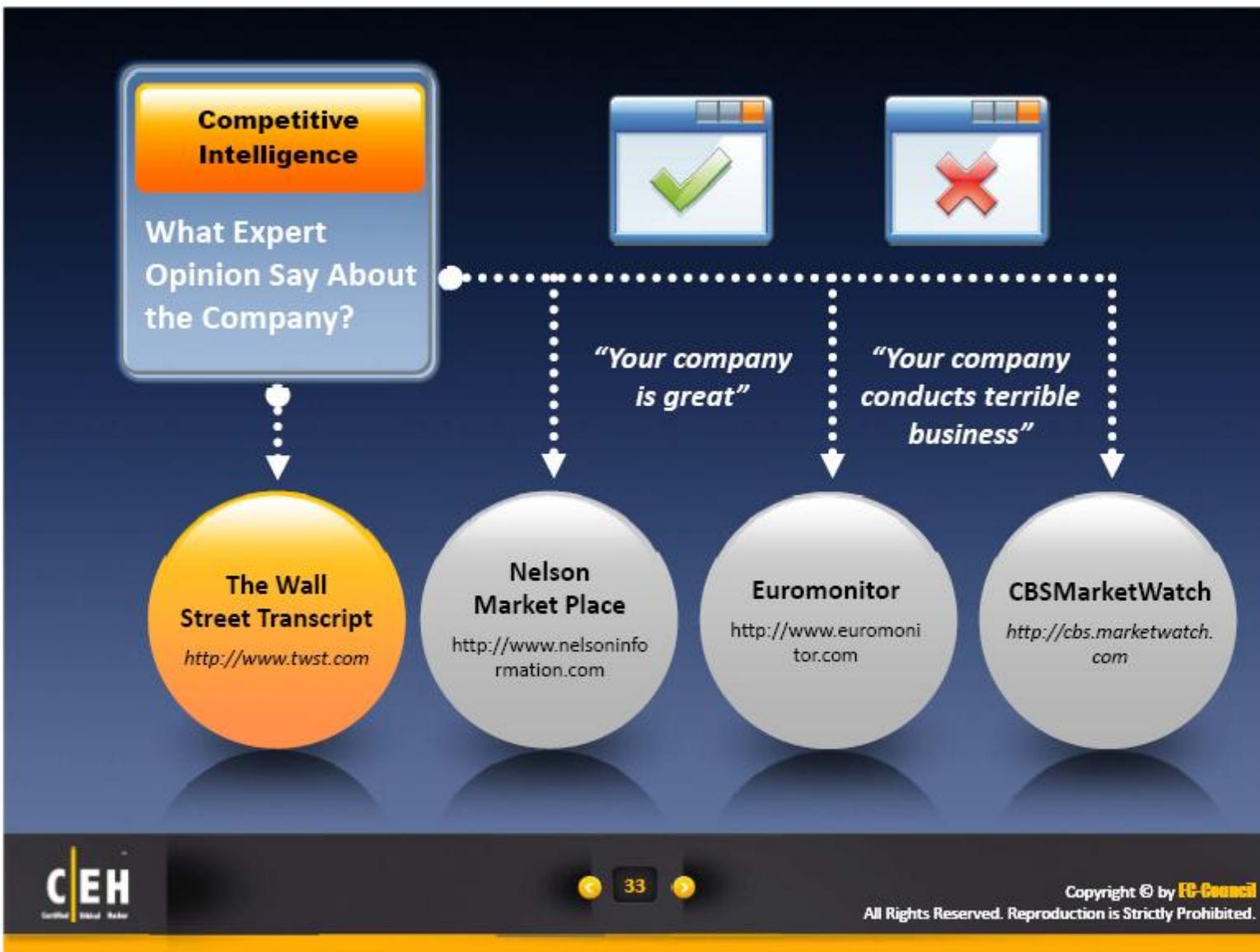
Competitive Intelligence Tools

SEC Info http://www.secinfo.com	**Business Wire** http://home.businesswire.com
C-SPAN http://www.cspan.org	**ChoicePoint Online** http://www.choicepointonline.com
CNN Money Company Research http://money.cnn.com	**Web Investigator** http://www.web-investigator.net
Forbes 500 http://www.forbes.com	**Barrons** http://online.barrons.com

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Competitive Intelligence Consulting Companies

http://www.carratu.com

http://www.fuld.com

http://www.globalintelligence.com

http://www.datamonitor.com

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting **Methodology**

Internet Footprinting

Competitive Intelligence

WHOIS Footprinting

DNS Footprinting

Network Footprinting

Website Footprinting

E-mail Footprinting

Google Hacking

WHOIS Lookup

WHOIS databases are maintained by Regional Internet Registries and contain the **personal information of domain owners**

WHOIS Query Returns

1. Domain name details
2. Contact details of domain owner
3. Domain name servers
4. NetRange

WHOIS Lookup Tools

http://www.tamos.com
http://netcraft.com
http://www.whois.net
http://www.iptools.com

Regional Internet Registry

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

Attackers Look for

1. Physical location
2. Telephone number
3. Email address
4. Technical and administrative contacts

CEH
Certified Ethical Hacker

37

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

WHOIS Lookup Result Analysis

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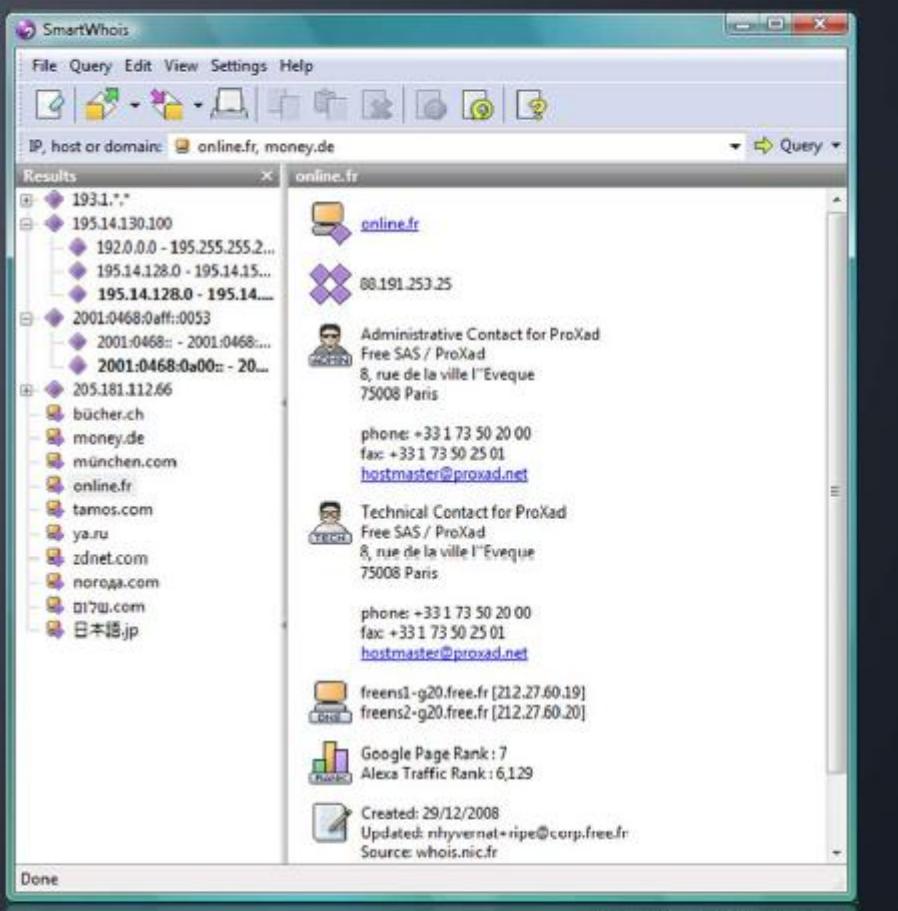
Technical Contact:
Surname, Name (SNIDNo-ORG)   targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

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

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

WHOIS Lookup Tools: SmartWhois

- SmartWhois is a useful network information utility that allows you to look up all the available information about an **IP address**, **hostname**, or **domain**

- It also provides information about **country**, **state or province**, **city**, name of the network provider, administrator, and technical support contact information

http://www.tamos.com

CEH

39

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

WHOIS Lookup Tools

Sam Spade
http://samspade.org

CountryWhois
http://www.tamos.com

NetRanger Whois
http://www.conceiva.com

Alchemy Eye
http://www.alchemy-lab.com

My IP Suite
http://www.sabsoft.com

LanWhois
http://lantricks.com

Lapshins Whois
http://lapshins.com

WebFerret
http://www.webferret.com

http://ceh.vn

CEH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

WHOIS Lookup Online Tools

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 **Methodology**

Internet Footprinting

Competitive Intelligence

WHOIS Footprinting

DNS Footprinting

Network Footprinting

Website Footprinting

E-mail Footprinting

Google Hacking

CEH

42

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
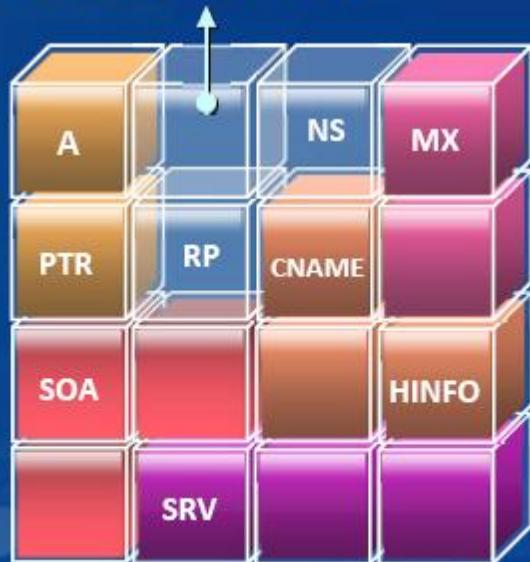
Extracting DNS Information

DNS Record Type

DNS Records provide important information about location and type of servers

- **A** - Points to a host's IP address
- **MX** - Points to domain's mail server
- **NS** - Points to host's name server
- **CNAME** - Canonical naming allows aliases to a host
- **SOA** - Indicate authority for domain
- **SRV** - Service records
- **PTR** - Maps IP address to a hostname
- **RP** - Responsible person
- **HINFO** - Host information record includes CPU type and OS

DNS Interrogation Tools
- http://www.dnsstuff.com
- http://network-tools.com
- http://www.checkdns.net
- http://www.iptools.com

CEH

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Extracting DNS Information

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

- Found NS record: ns1.msft.net[65.55.37.62], was resolved to IP address by e.gtld-servers.net
- Found NS record: ns2.msft.net[64.4.59.173], was resolved to IP address by e.gtld-servers.net
- Found NS record: ns3.msft.net[213.199.161.77], was resolved to IP address by e.gtld-servers.net
- Found NS record: ns4.msft.net[207.46.75.254], was resolved to IP address by e.gtld-servers.net
- 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

- DNS server ns1.msft.net[65.55.37.62] is alive and authoritative for domain microsoft.com
- DNS server ns2.msft.net[64.4.59.173] is alive and authoritative for domain microsoft.com
- DNS server ns3.msft.net[213.199.161.77] is alive and authoritative for domain microsoft.com
- DNS server ns4.msft.net[207.46.75.254] is alive and authoritative for domain microsoft.com
- 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

http://www.checkdns.net

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

DNS Interrogation Tools

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

http://ceh.vn

CEH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

DNS Interrogation Online Tools

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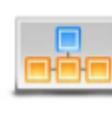
Domain Information Groper
http://www.kloth.net

Locate the Network Range

TARGET

01000101101011111001010

1. **Find the range of IP addresses**
2. **Use ARIN whois database search tool**

You can find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR)
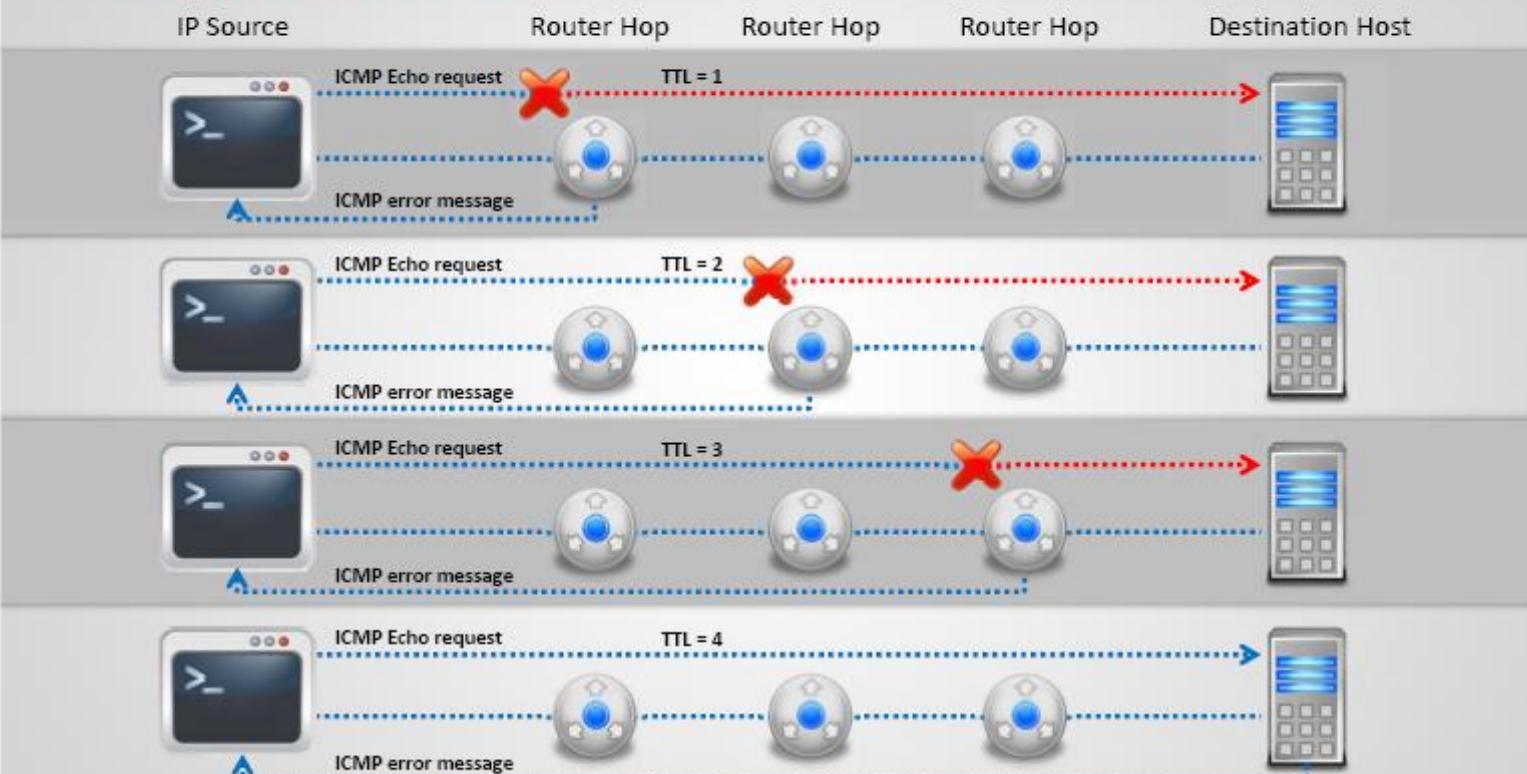
Network Whois record

```
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
OrgAbusePhone:     +1-425-882-8080
OrgAbuseEmail:     abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

CEH

48

Traceroute

Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host

Traceroute Analysis

I — Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations

**II** — For example: after running several traceroutes, an attacker might obtain the following information:

- 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
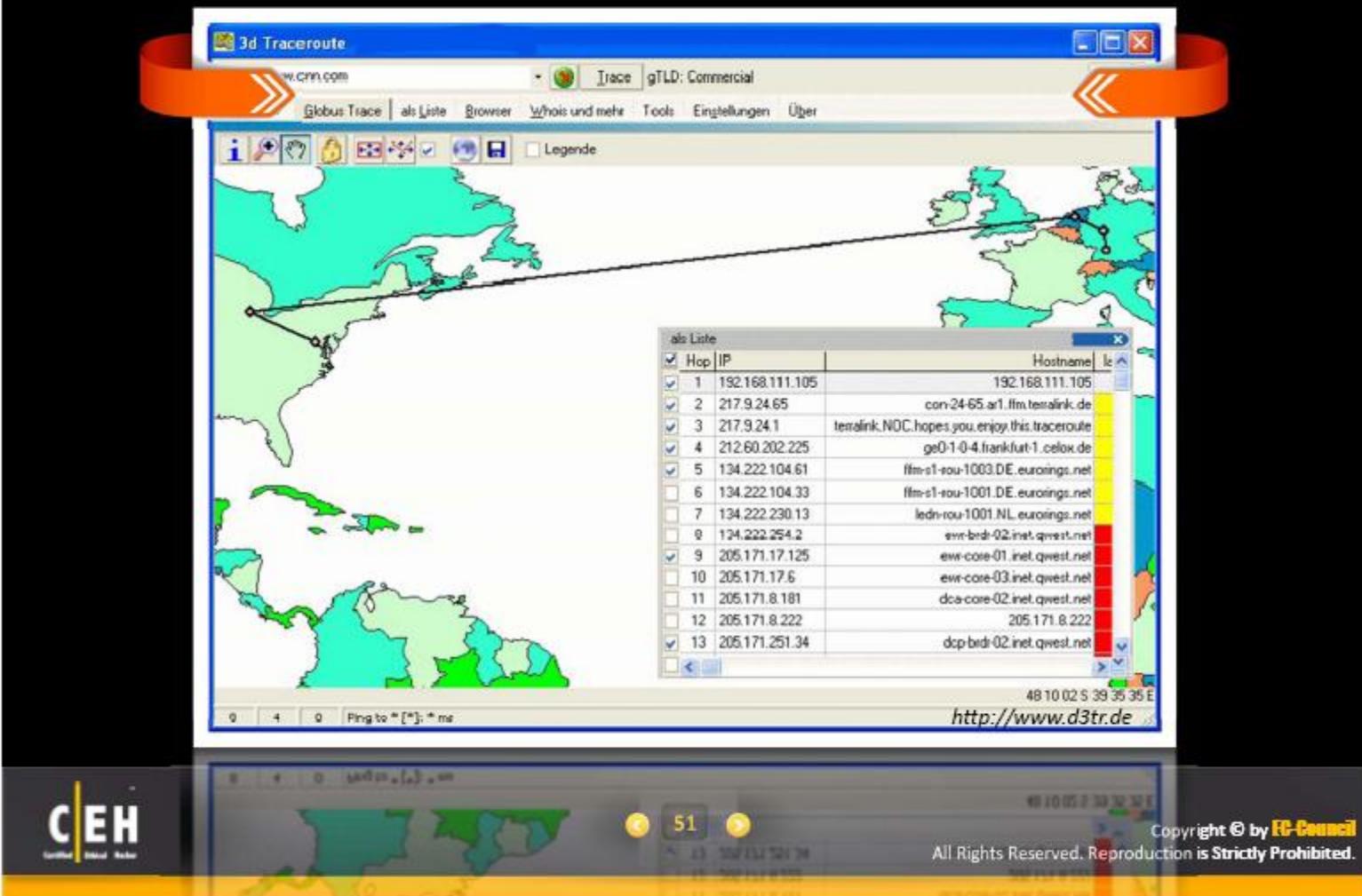
III — By putting this information together, attackers can draw the network diagram

20.20.10.20
Bastion Host

1.10.20.10
Web Server

Hacker

1.10.10.1
Router

1.10.10.50
Firewall

1.10.20.15
Mail Server

DMZ ZONE

1.10.20.50
Firewall

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Traceroute Tool: 3D Traceroute

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services
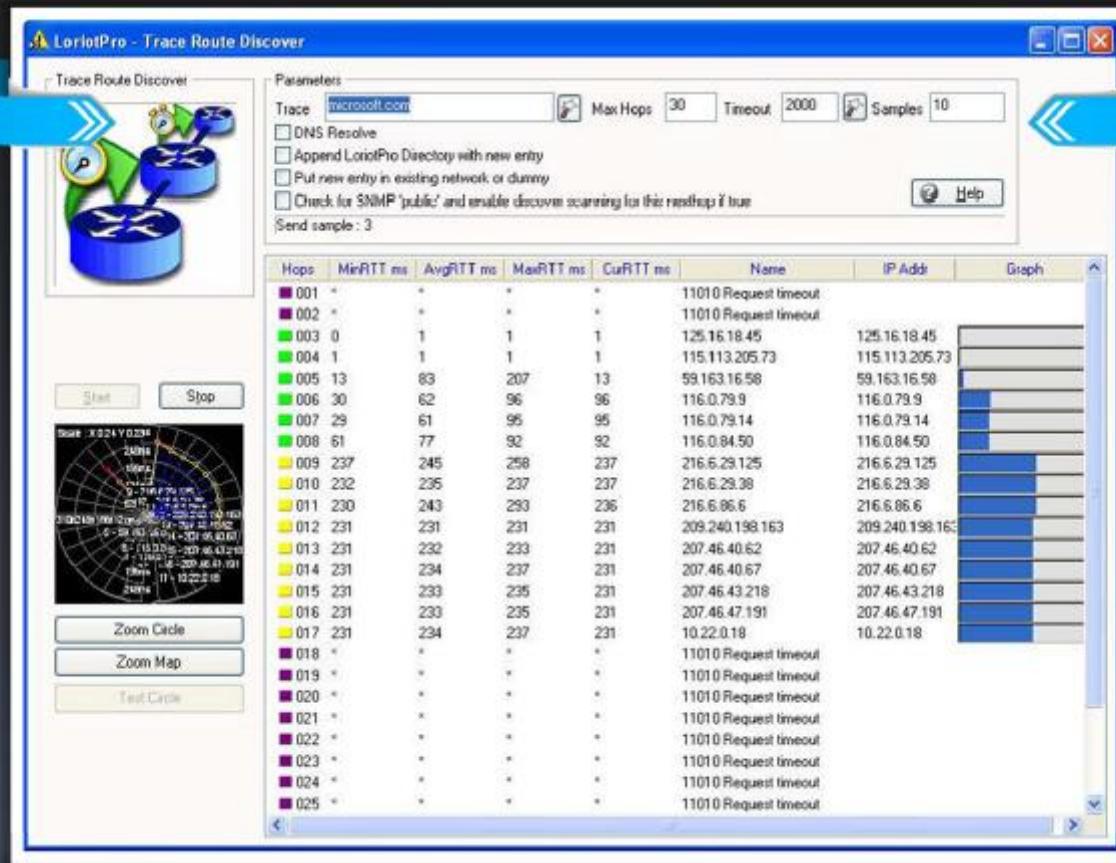
http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Traceroute Tool: LoriotPro
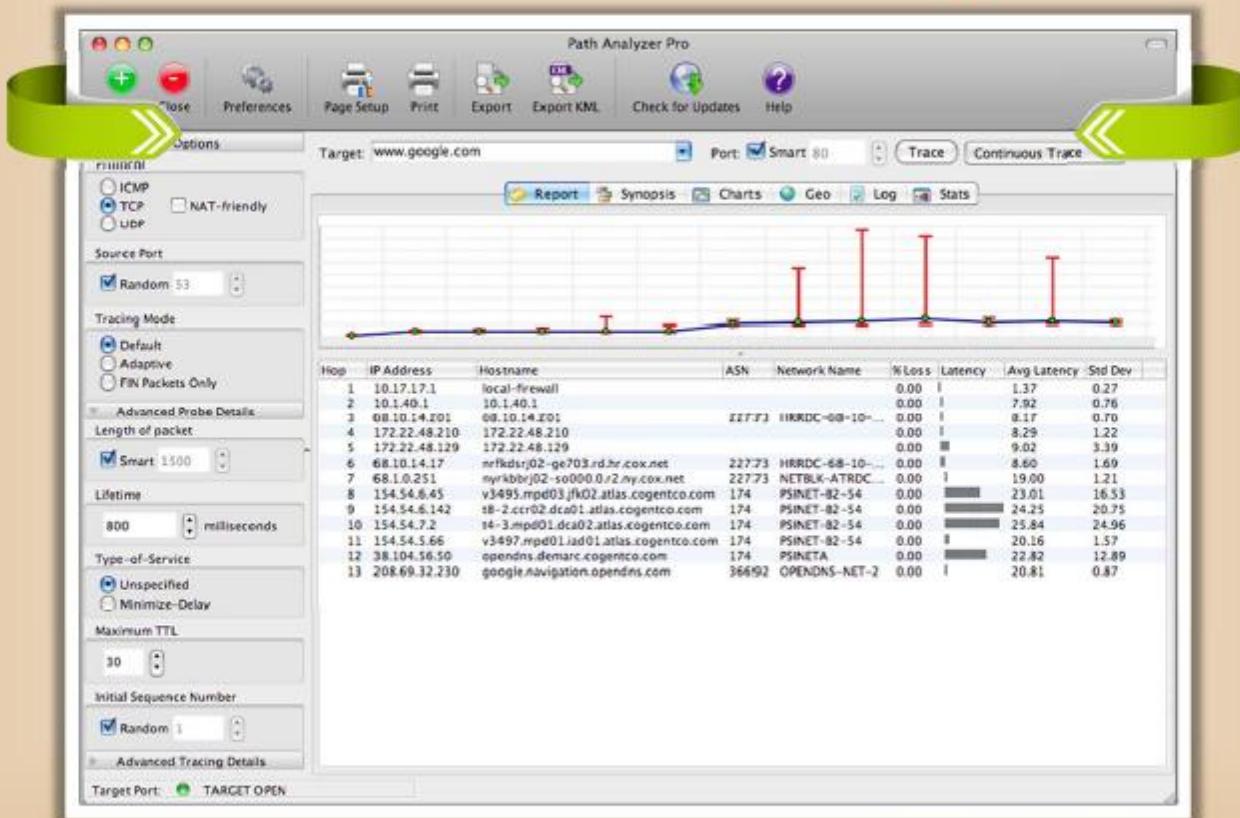
Traceroute Tool: Path Analyzer Pro

http://www.pathanalyzer.com

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Traceroute Tools

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

Traceroute Tools

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
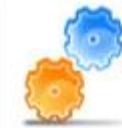
Network Systems Traceroute
http://www.net.princeton.edu
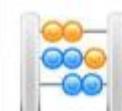
Tracepath
http://whatismyipaddress.com

Roadkil's Trace Route
http://www.roadkil.net

Ping-Probe
http://www.ping-probe.com

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
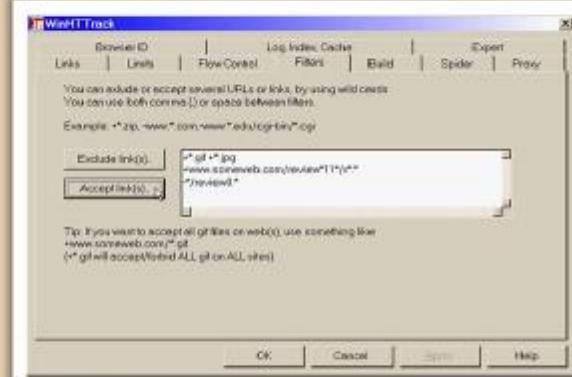
Mirroring Entire Website

Web mirroring tools allows you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos and other files from the server to your computer

Original Website

Mirrored Website

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
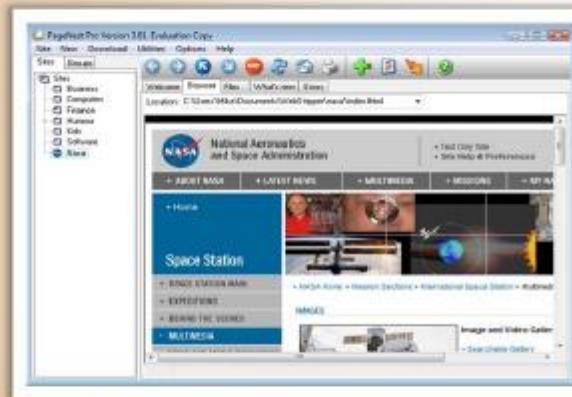
Website Mirroring Tools

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

SurfOffline (*http://www.surfoffline.com*)

PageNest (*http://www.pagenest.com*)

KeepNI (*http://www.keepni.com*)

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Mirroring Entire Website Tools

Wget
http://www.gnu.org

Website Ripper Copier
http://www.tensons.com
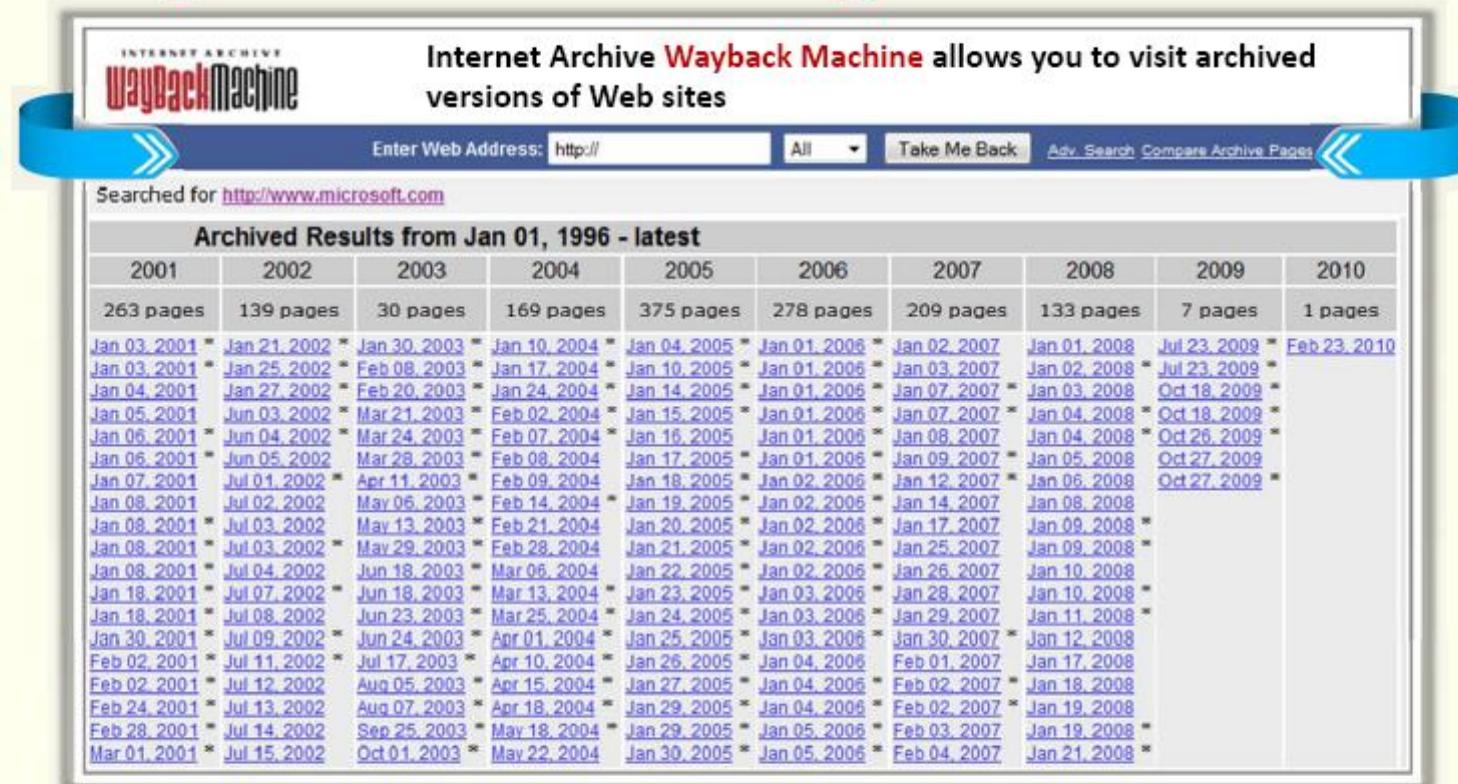
Webripper
http://calluna-software.com

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

http://ceh.vn

EH NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Extract Website Information from
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 *		
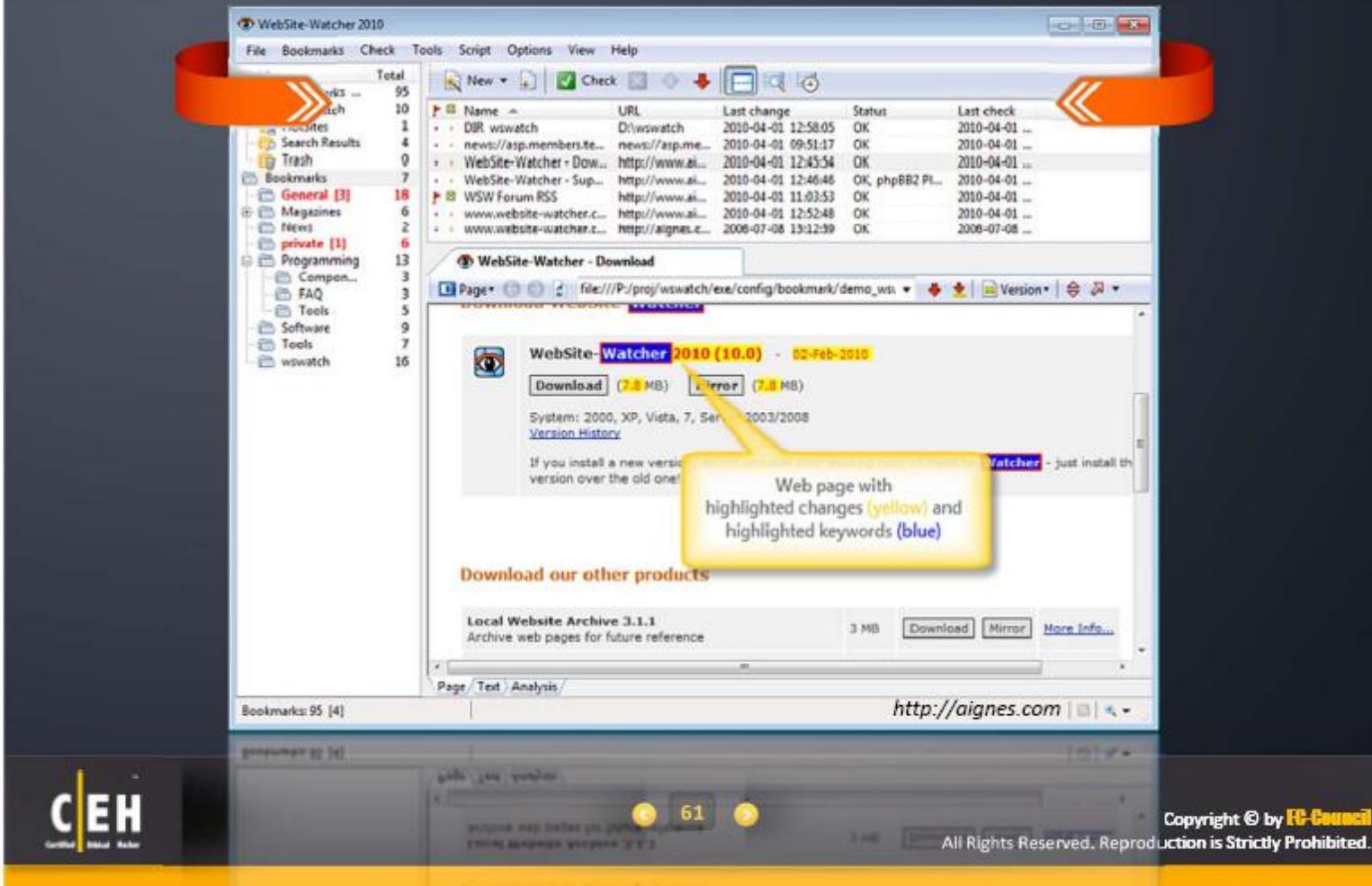
CEH
Certified Ethical Hacker

◄ 60 ►

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Monitoring Web Updates Using Website Watcher

61

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Tracking **Email Communications**

E-mail tracking is a method to monitor and spy the delivered e-mails **to the intended recipient**

01	When the email was received and read
02	Send destructive emails
03	GPS location and map of the recipient
04	Time spent on reading the emails
05	Whether or not the recipient visited any links sent to them
06	Track PDF and other types of attachments
07	Set messages to expire after a specified time

Email Tracking

CEH

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Email Tracking Tools

eMailTrackerPro
http://www.emailtrackerpro.com

Read Notify
http://www.readnotify.com

DidTheyReadIt
http://www.didtheyreadit.com

PoliteMail
http://www.politemail.com

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design
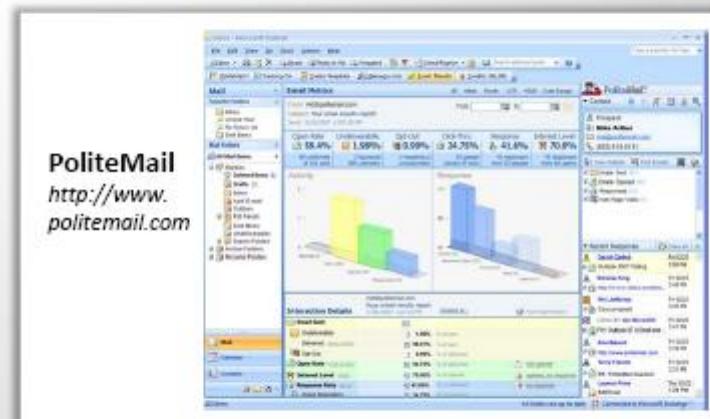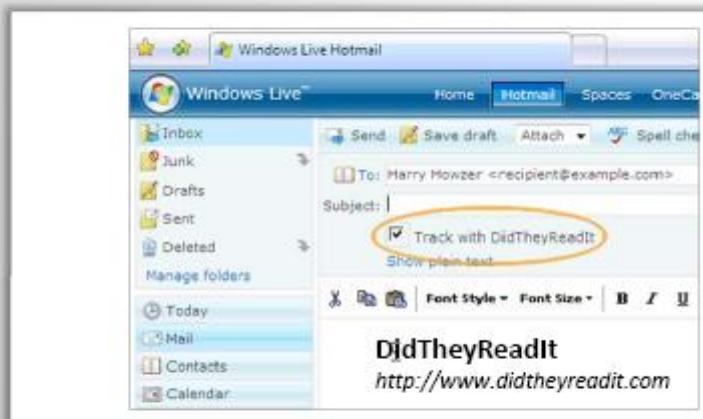
Email Tracking Tools

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

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprint Using Google Hacking Techniques

Query String

Google hacking is a term that refers to the art of creating complex **search engine queries**

Vulnerable Sites

It detects websites that are **vulnerable** to numerous exploits and vulnerabilities

Google Operators

It uses Google operators to **locate specific strings of text** within the search results

Google Advance Search Operators

Google supports several advanced operators that help in modifying the search

[cache:]	Shows the version of the web page that Google has in its cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are "similar" to a specified web page.
[info:]	Will present some information that Google has about that web page
[site:]	If you include [site:] in your query, Google restricts the results to those websites in the given domain
[allintitle:]	If you start a query with [allintitle:], Google restricts the results to those with all of the query words in the title
[intitle:]	If you include [intitle:] in your query, Google restricts the results to documents containing that word in the title
[allinurl:]	If you start a query with [allinurl:], Google restricts the results to those with all of the query words in the url
[inurl:]	If you include [inurl:] in your query, Google restricts the results to documents containing that word in the url

Finding Resources using Google Advance Operator

[intitle:intranet inurl:intranet +intext:"human resources"]:

It allows you not only to access a company's private network, but also provides the **employee listings** and other **sensitive information** that can be incredibly useful for any social engineering endeavor

Google

Web   Images   Videos   Maps   News   Shopping   Gmail   more ▼   Sign in

Google   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

Google Hacking Tool: Google Hacking Database (GHDB)

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Google Hacking Tools

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

Module Flow

Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

Footprinting Countermeasures

Footprinting Pen Testing

http://ceh.vn

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Additional Footprinting Tools

	Prefix WhoIs *http://pwhois.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*

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Additional Footprinting Tools

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

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Additional Footprinting Tools

Touchgraph
http://www.touchgraph.com

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

Spyfu
http://www.spyfu.com

CallerIP
http://www.callerippro.com

ActiveWhois
http://www.johnru.com

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

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

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

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting **Countermeasures**

1. Configure routers to restrict the responses to footprinting requests

2. Configure web servers to avoid information leakage and disable unwanted protocols

3. Lock the ports with the suitable firewall configuration

4. Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns

5. Evaluate the information before publishing it on the website/Internet

6. Perform footprinting techniques and remove any sensitive information found

7. Prevent search engines from caching a webpage and use anonymous registration services

8. Disable directory listings and use split-DNS

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Module Flow

Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

Footprinting Countermeasures

Footprinting Pen Testing

CEH
Certified Ethical Hacker

79

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting Pen Testing

- Footprinting pen test is used to determine **organization's publicly available information on the Internet** such as network architecture, operating systems, applications and users

- The tester attempts to gather as much information as possible about the target organization from **internet and other publicly accessible sources**

Prevent **information leakage**

Footprinting Pen testing helps administrator to:

Prevent **DNS record retrieval** from publically available servers

Prevent **social engineering attempts**

CEH
Certified Ethical Hacker

http://ceh.vn

NEWS
Certified Ethical Hacker

I-TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting Pen Testing

START ····▶

- **Get proper authorization**
- **Define the scope of the assessment**
- **Perform Internet footprinting** ····▶ Use tools such as Web Data Extractor, Link Extractor, etc.
- **Gather competitive intelligence** ····▶ Use tools such as SEC Info, Business Wire, C-SPAN, etc.
- **Perform WHOIS fingerprinting** ····▶ Use tools such as SmartWhois, Alchemy Eye, etc.

- Get proper authorization and define the scope of the assessment
- Perform Internet footprinting using tools such as Web Data Extractor, Link Extractor, etc
- Gather Competitive intelligence using tools such as SEC Info, Business Wire, C-SPAN, etc
- Perform WHOIS fingerprinting using tools such as SmartWhois, Alchemy Eye, etc

http://ceh.vn

NEWS Certified Ethical Hacker

I-TRAIN Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Footprinting Pen Testing

Perform email footprinting
Use tools such as NetInspector, NsLookup, etc.

Perform website footprinting
Use tools such as 3D Traceroute, LoriotPro, etc.

Perform network footprinting
Use tools such as HTTrack Web Site Copier, Wget, etc.

Perform DNS footprinting
Use tools such as eMailTrackerPro, PoliteMail, etc.

Perform Google hacking
Use tools such as GHDB, MetaGoofil, SiteDigger, etc.

Document all the findings

- Perform email footprinting using tools such as NetInspector, NsLookup, etc.

- Perform website footprinting using tools such as 3D Traceroute, LoriotPro, etc.

- Perform network footprinting using tool such as HTTrack Web Site Copier, Wget, etc.

- Perform DNS footprinting using tools such as eMailTrackerPro, PoliteMail, etc.

- Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc.

- At the end of pen testing document all the findings

CEH

82

http://ceh.vn

EH NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Module **Summary**

- ❑ Footprinting refers to uncovering and collecting as much information as possible about a target of attack

- ❑ WHOIS databases are maintained by Regional Internet Registries and contains the personal information of domain owners

- ❑ DNS Records provide important information about location and type of servers

- ❑ Personal information can be found using online people search services

- ❑ You can establish email communication with the target company and track the emails to extract information such as location of the recipient and mail servers

- ❑ Competitive intelligence gathering is the process of gathering information about your competitors from resources such as the Internet

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design

Quotes

> **"** If you know the enemy and know yourself you need not fear the results of a hundred battles **"**

– **Sun Tzu,**
Ancient Chinese
Strategist and
Philosopher

http://ceh.vn

NEWS
Certified Ethical Hacker

I - TRAIN
Professional Training Services

http://i-train.com.vn
CEH, MCITP, CCNA, CCNP, VMware sPhere, LPI, Web Design