# Footprinting and Reconnaissance

## Module 2

Engineered by Hackers. Presented by Professionals.

# SECURITY NEWS

21st May 2010, Chicago, Illinois

iTWeb

## 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.

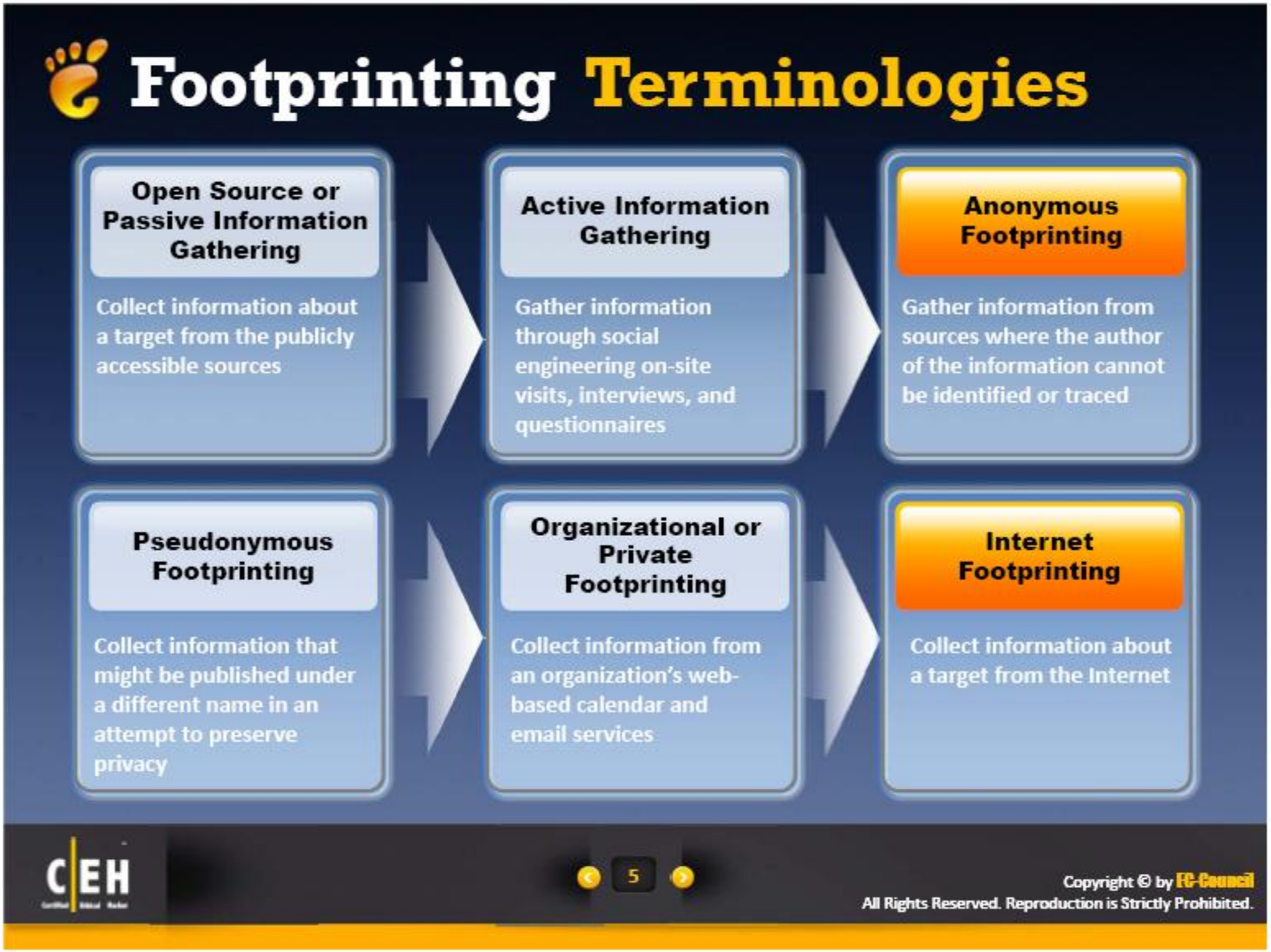
*http://www.itweb.co.za*

# 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



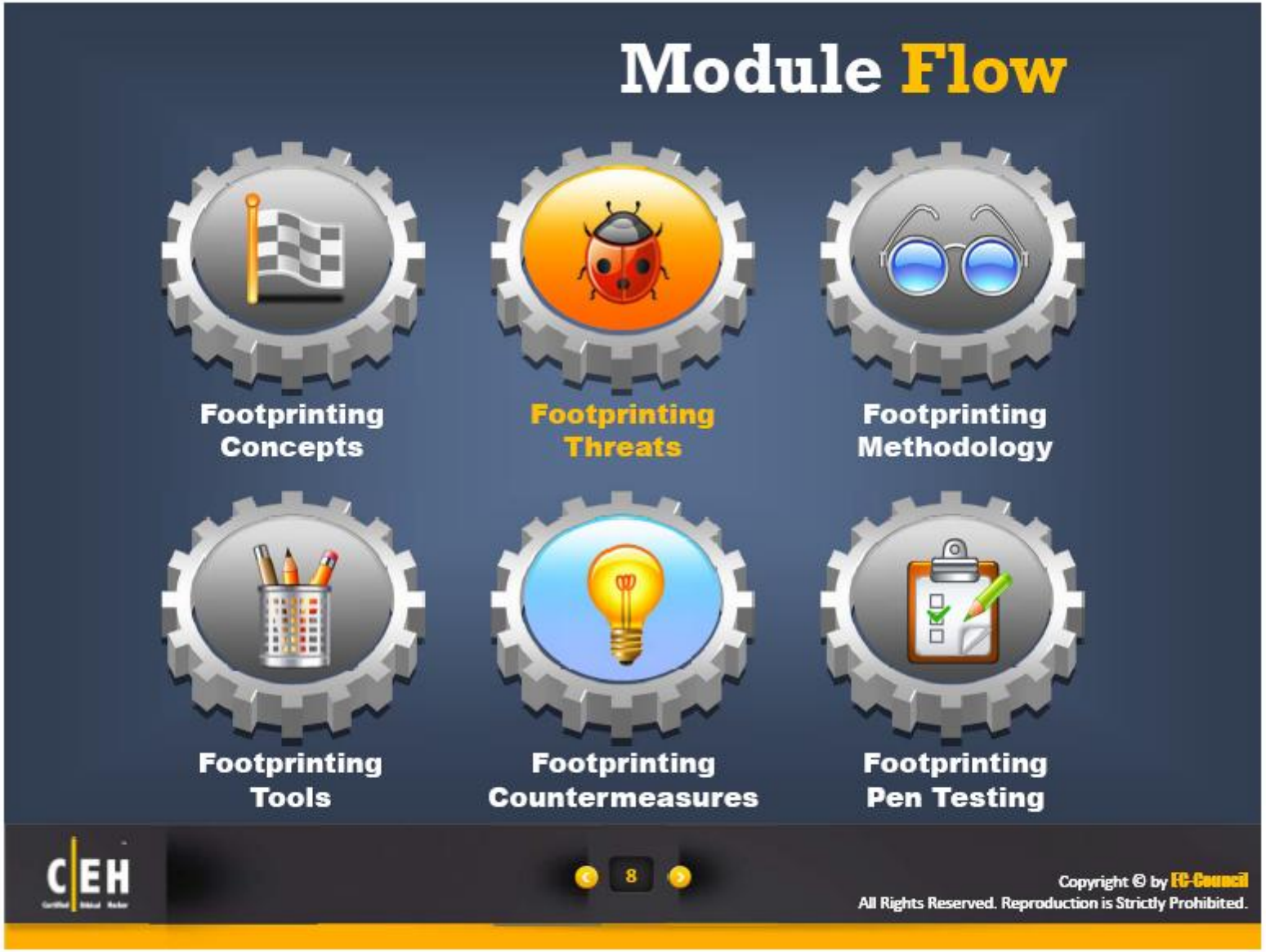


# What is Footprinting?

Footprinting refers to **uncovering** and **collecting** as much **information** as possible about a target network

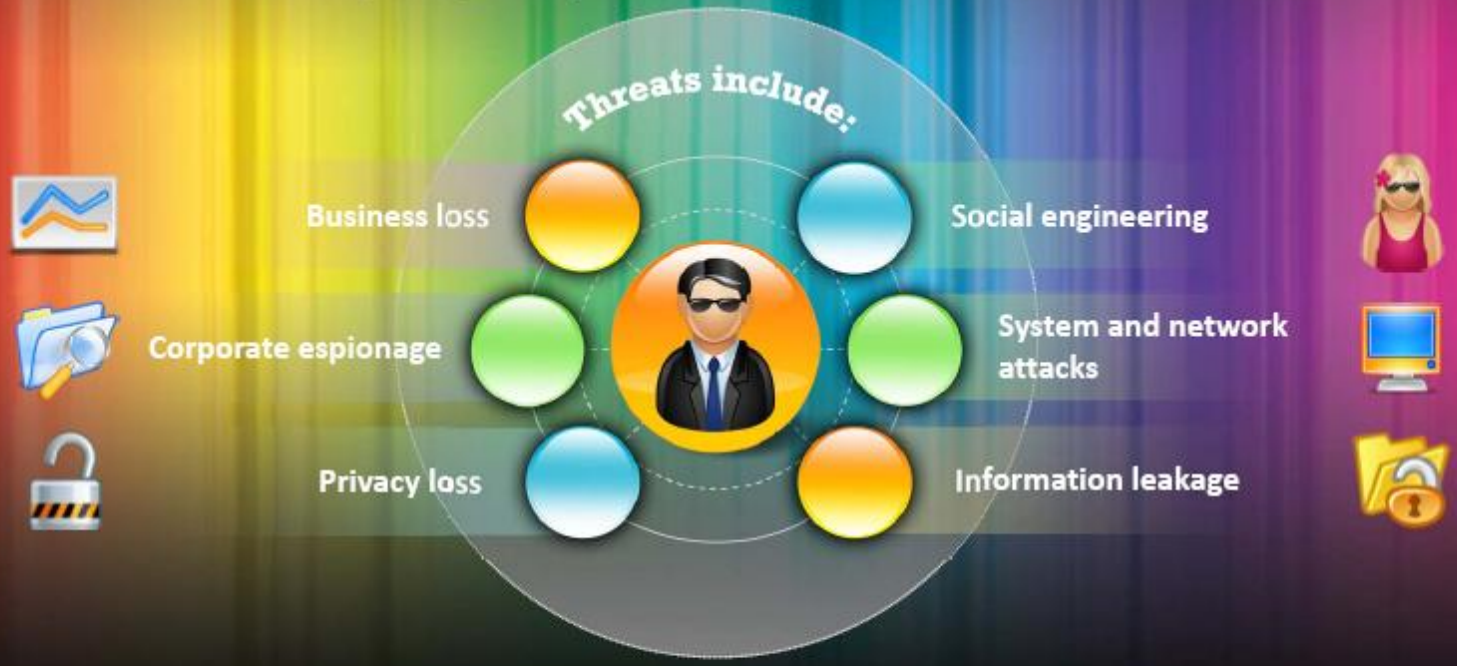
# Objectives of Footprinting

| | | |
|---|---|---|
|  **Collect Network Information** | ▪ Domain name<br>▪ Internal domain names<br>▪ Network blocks<br>▪ IP addresses of the reachable systems<br>▪ Rogue websites/private websites<br>▪ TCP and UDP services running | ▪ Networking protocols<br>▪ VPN Points<br>▪ ACLs<br>▪ IDSes running<br>▪ Analog/digital telephone numbers<br>▪ Authentication mechanisms |
|  **Collect System Information** | ▪ User and group names<br>▪ System banners<br>▪ Routing tables<br>▪ SNMP information | ▪ System architecture<br>▪ Remote system type<br>▪ System names<br>▪ Passwords |
|  **Collect Organization's Information** | ▪ Employee details<br>▪ Organization's website<br>▪ Company directory | ▪ Address and phone numbers<br>▪ Background on the organization<br>▪ News articles/press releases |


Module Flow
Footprinting Concepts
Footprinting Threats
Footprinting Methodology
Footprinting Tools
Footprinting Countermeasures
Footprinting Pen Testing
CEH
8
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

# 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

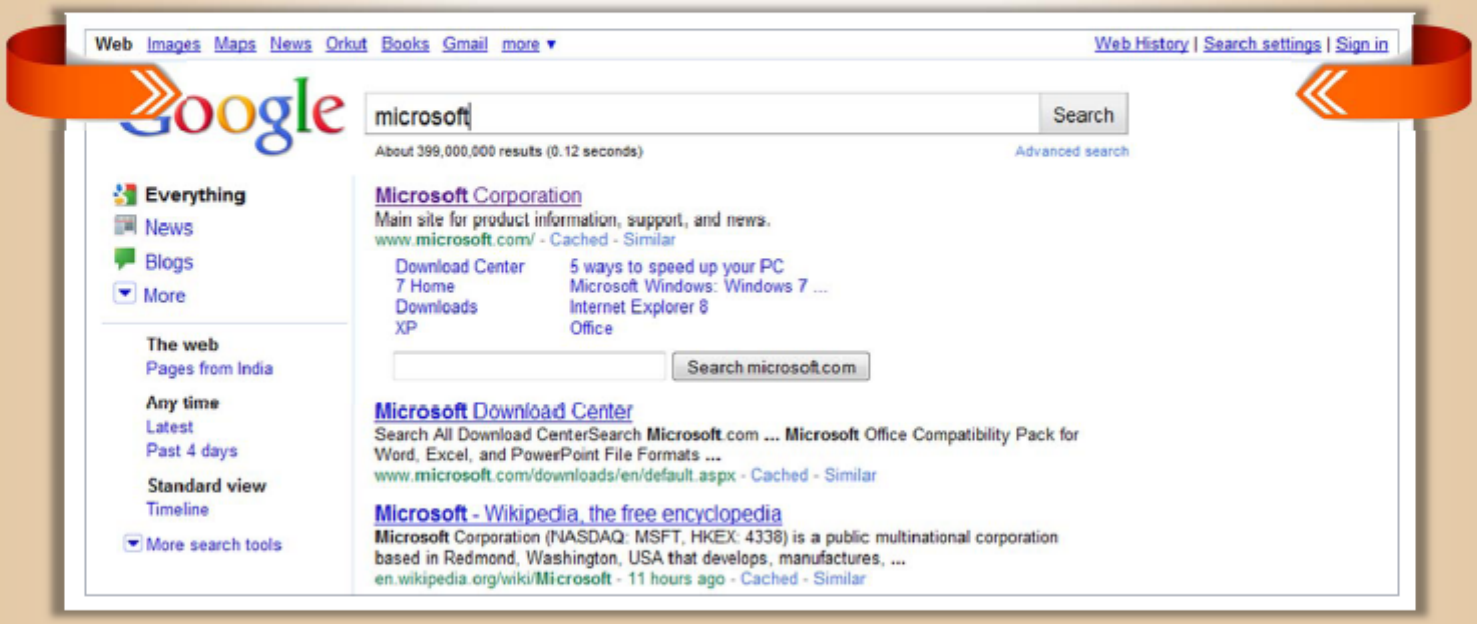



Module Flow
Footprinting Concepts
Footprinting Threats
Footprinting Methodology
Footprinting Tools
Footprinting Countermeasures
Footprinting Pen Testing
CEH
10
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

# Footprinting Methodology

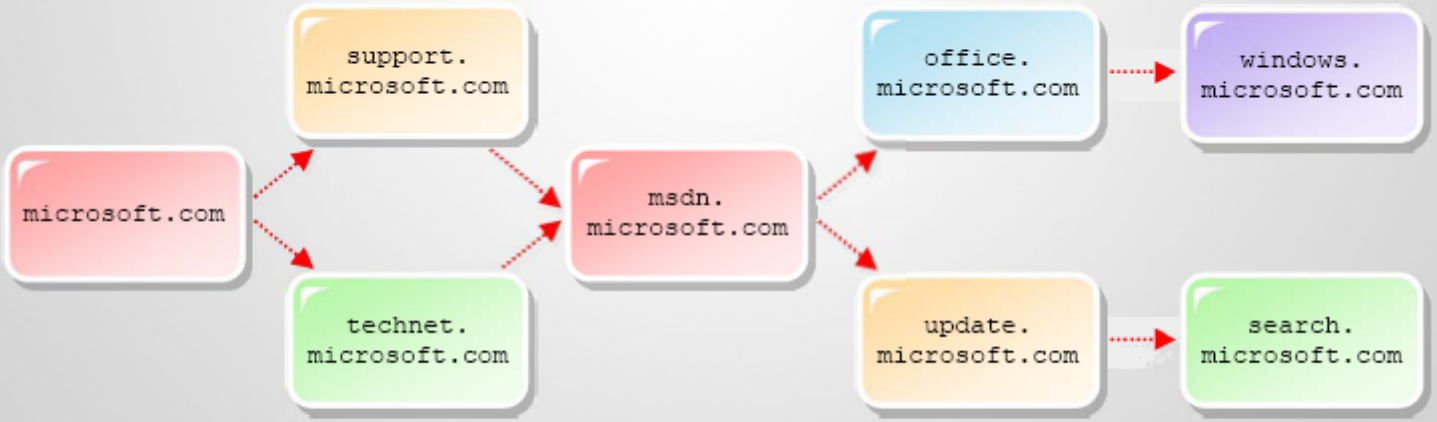
# Finding a Company's URL

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



# Locate Internal URLs

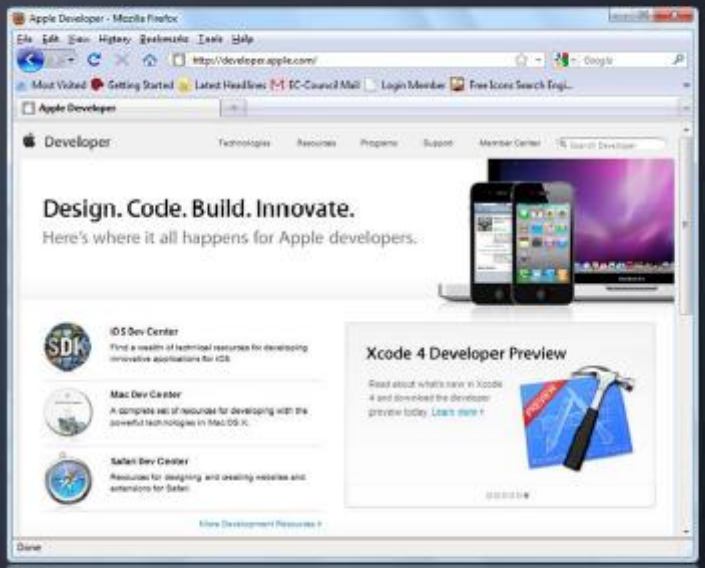
- Internal URLs **provide an insight** into different departments and business units in an organization
- You may find an internal company's URL **by trial and error method**
- **Tools** to search internal URLs:
  - *http://news.netcraft.com*
  - *http://www.webmaster-a.com/link-extractor-internal.php*



# Public and Restricted Websites

- Identify a company's private and public websites


Public website
*http://www.apple.com*




Restricted website
*http://developer.apple.com*

# 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

# 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*)

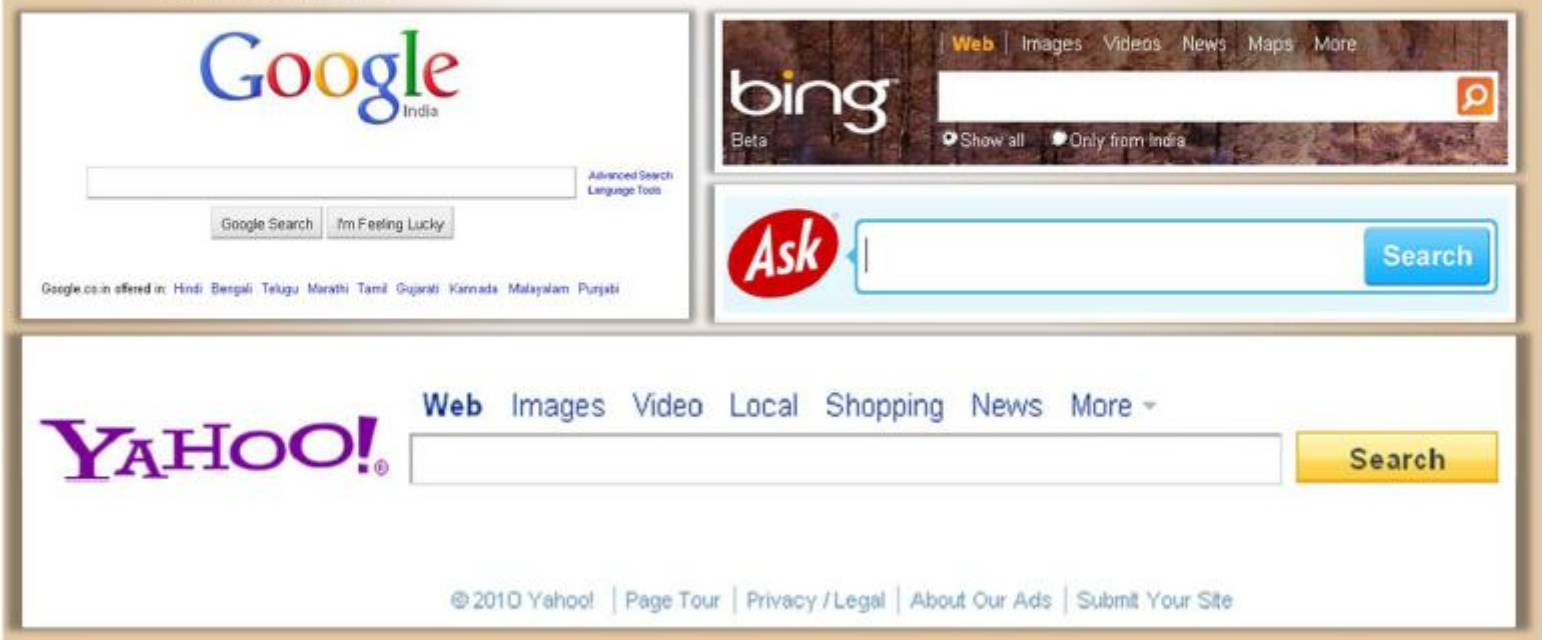
- SpiderFoot is a domain footprinting tool which will **scrape the websites** on that domain, as well as search Google, Netcraft, Whois, and DNS to collect the company information

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

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

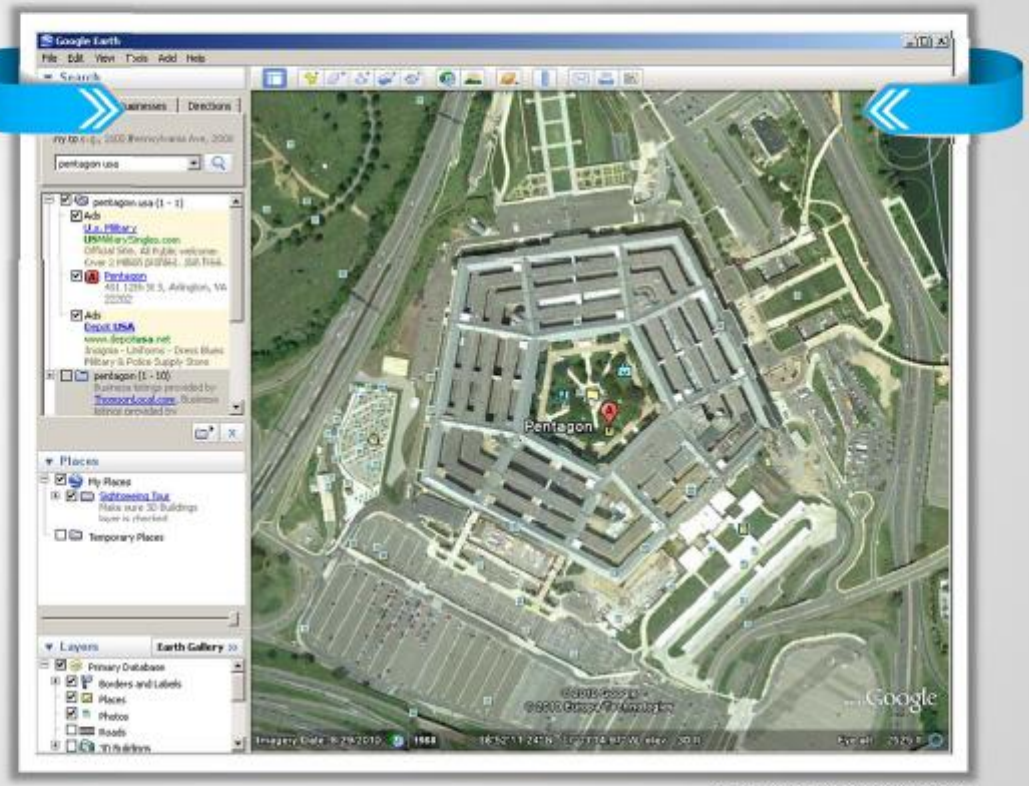
# Footprinting Through Search Engines

- 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)



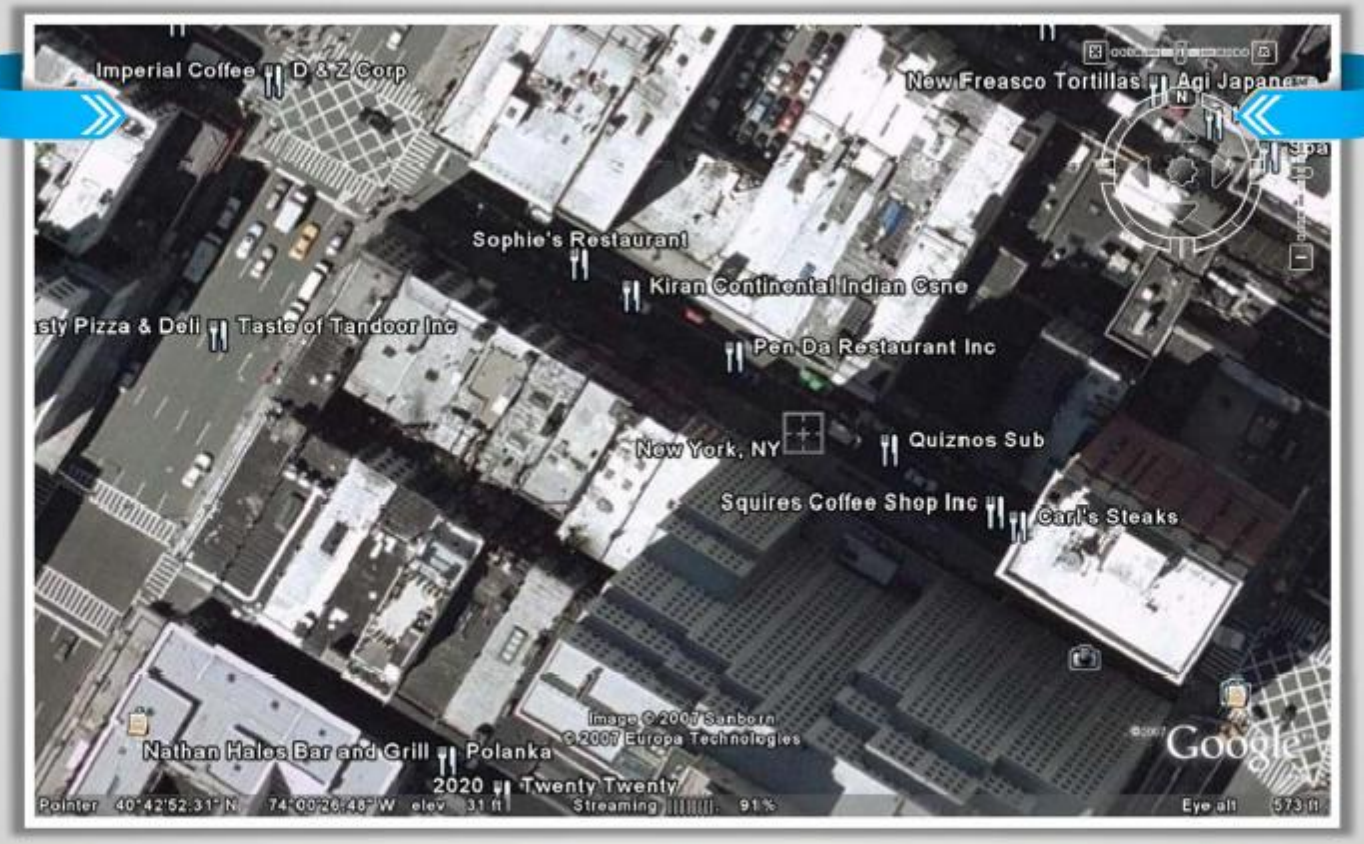
# Collect Location Information

- Use GoogleEarth tool to get the location of the place




http://earth.google.com

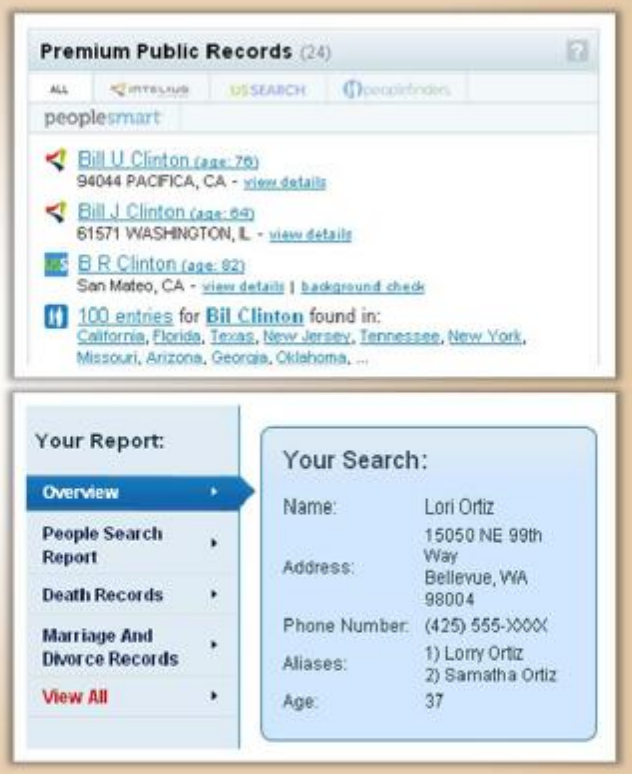
# Satellite Picture of a Residence



# 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




You can find personal information using online people search services

# 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

# 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*

# People Search on Social Networking Services


http://www.orkut.com


http://www.facebook.com


http://www.linkedin.com


http://twitter.com

# Gather Information from Financial Services

**Google Finance**

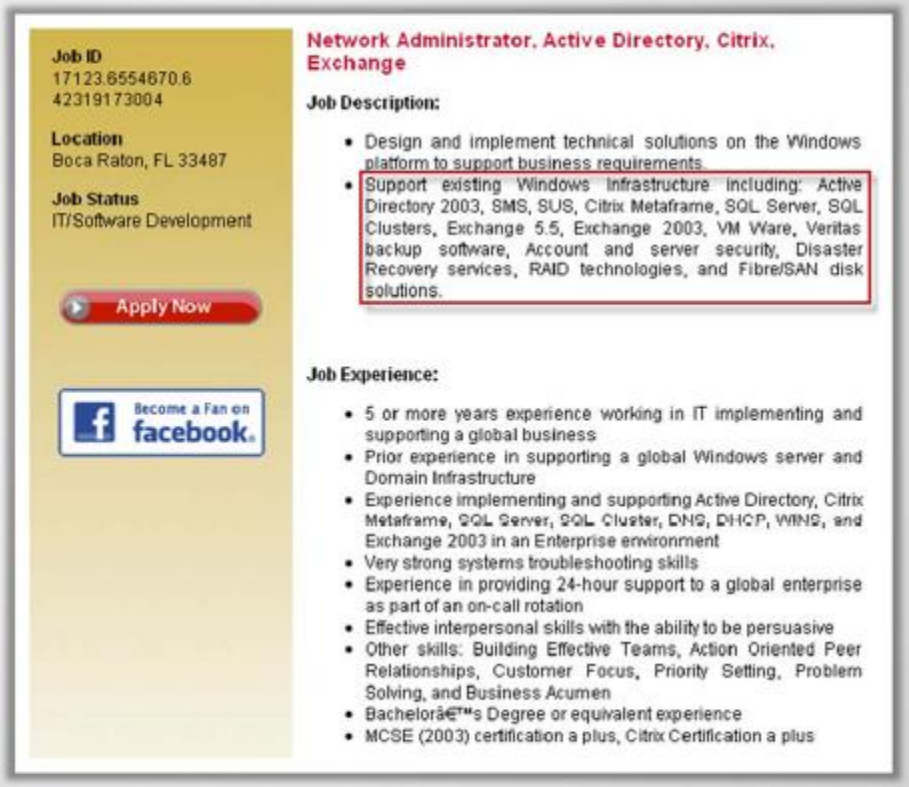

**Yahoo Finance**

# 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

Become a Fan on facebook.

**Network Administrator, Active Directory, Citrix, Exchange**

**Job Description:**

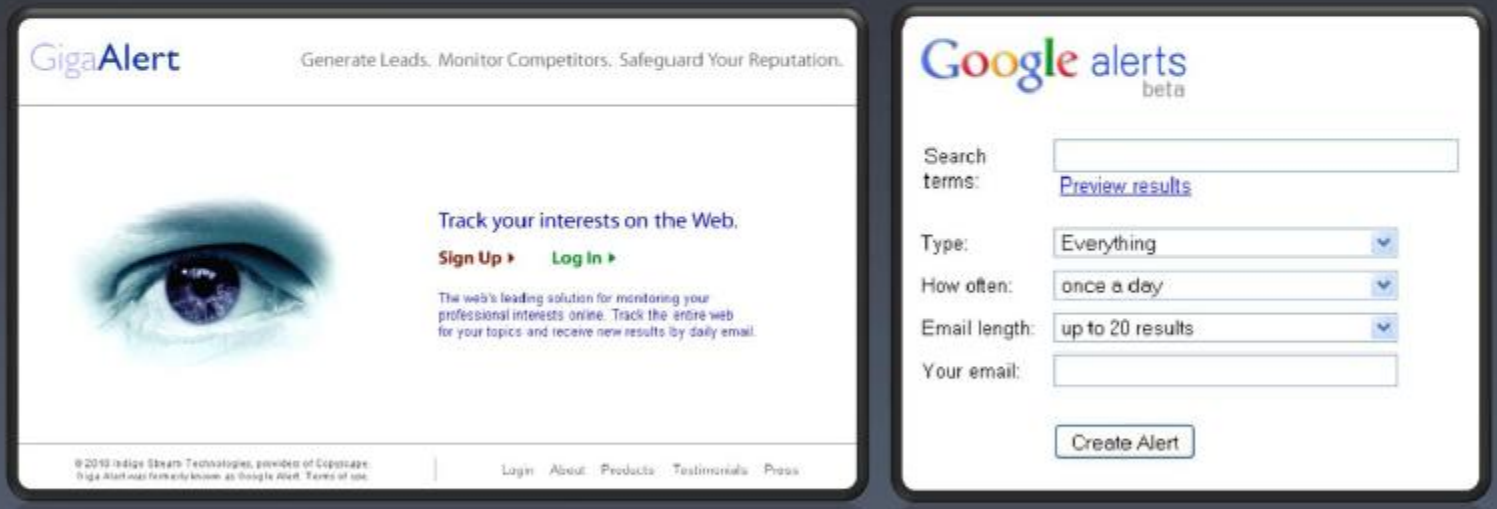
- Design and implement technical solutions on the Windows platform to support business requirements.
- Support existing Windows infrastructure including: Active Directory 2003, SMS, SUS, Citrix Metaframe, SQL Server, SQL Clusters, Exchange 5.5, Exchange 2003, VM Ware, Veritas backup software, Account 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

# 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



# Footprinting Methodology

# 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

# 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



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


## 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

# 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*)


Competitive Intelligence
What Expert Opinion Say About the Company?
"Your company is great"
"Your company conducts terrible business"
The Wall Street Transcript
http://www.twst.com
Nelson Market Place
http://www.nelsoninformation.com
Euromonitor
http://www.euromonitor.com
CBSMarketWatch
http://cbs.marketwatch.com
CEH
33
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

# 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*

# Competitive Intelligence Consulting Companies


http://www.carratu.com


http://www.fuld.com


http://www.globalintelligence.com


http://www.datamonitor.com


Footprinting Methodology
Internet Footprinting
Competitive Intelligence
WHOIS Footprinting
DNS Footprinting
Network Footprinting
Website Footprinting
E-mail Footprinting
Google Hacking
C|EH
36
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

# WHOIS Lookup

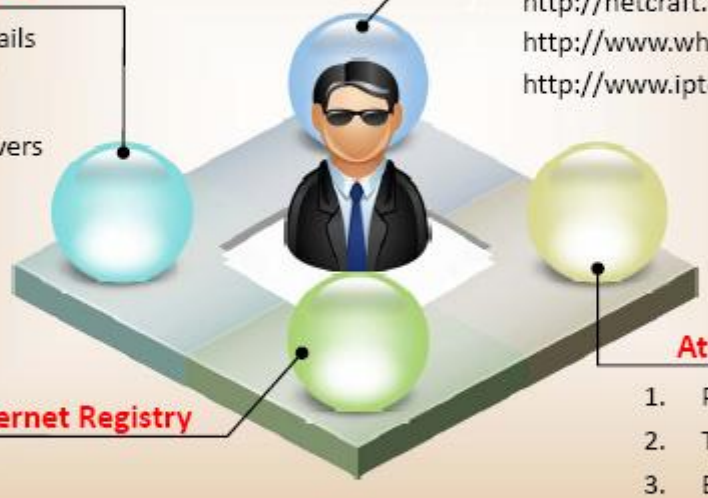
WHOIS databases are maintained by Regional Internet Registries and contain the **personal information of domain owners**

### WHOIS Lookup Tools

1. http://www.tamos.com
2. http://netcraft.com
3. http://www.whois.net
4. http://www.iptools.com

### WHOIS Query Returns

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



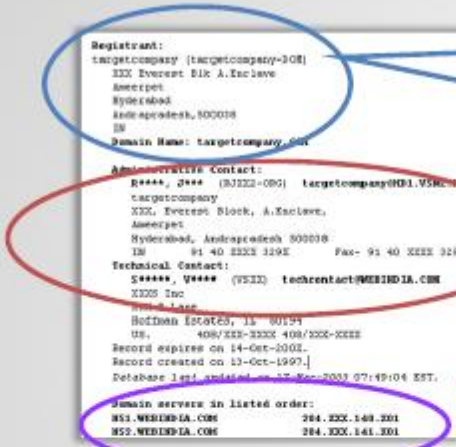
### Regional Internet Registry

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

# WHOIS Lookup Result Analysis



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

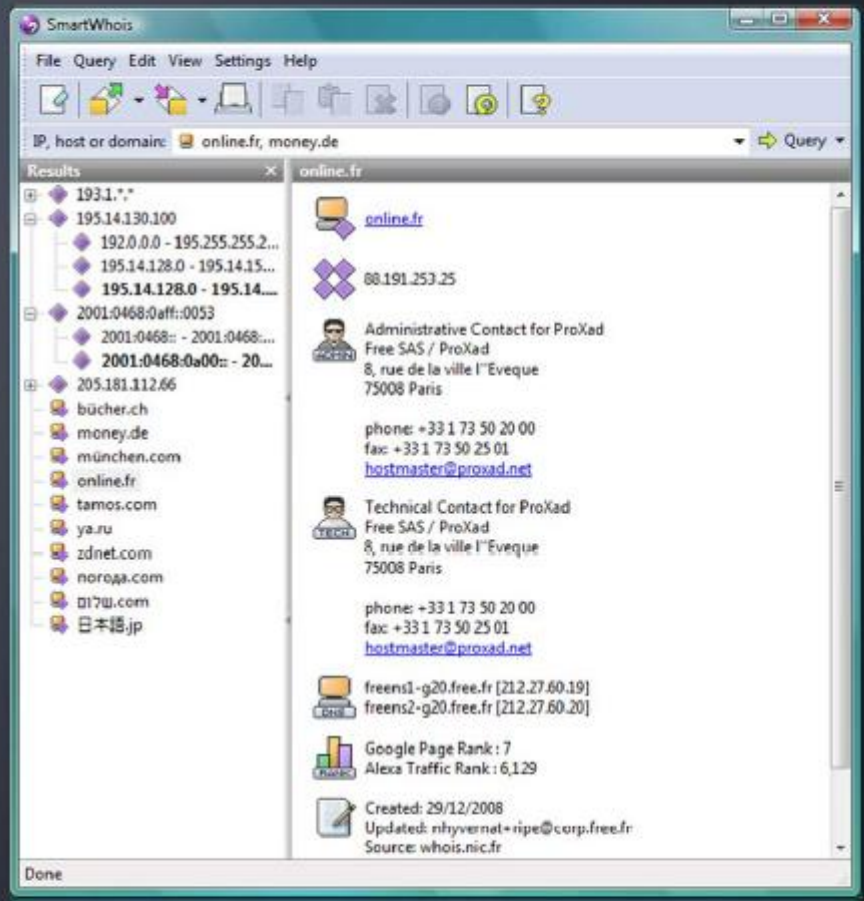
**Administrative Contact:**
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

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

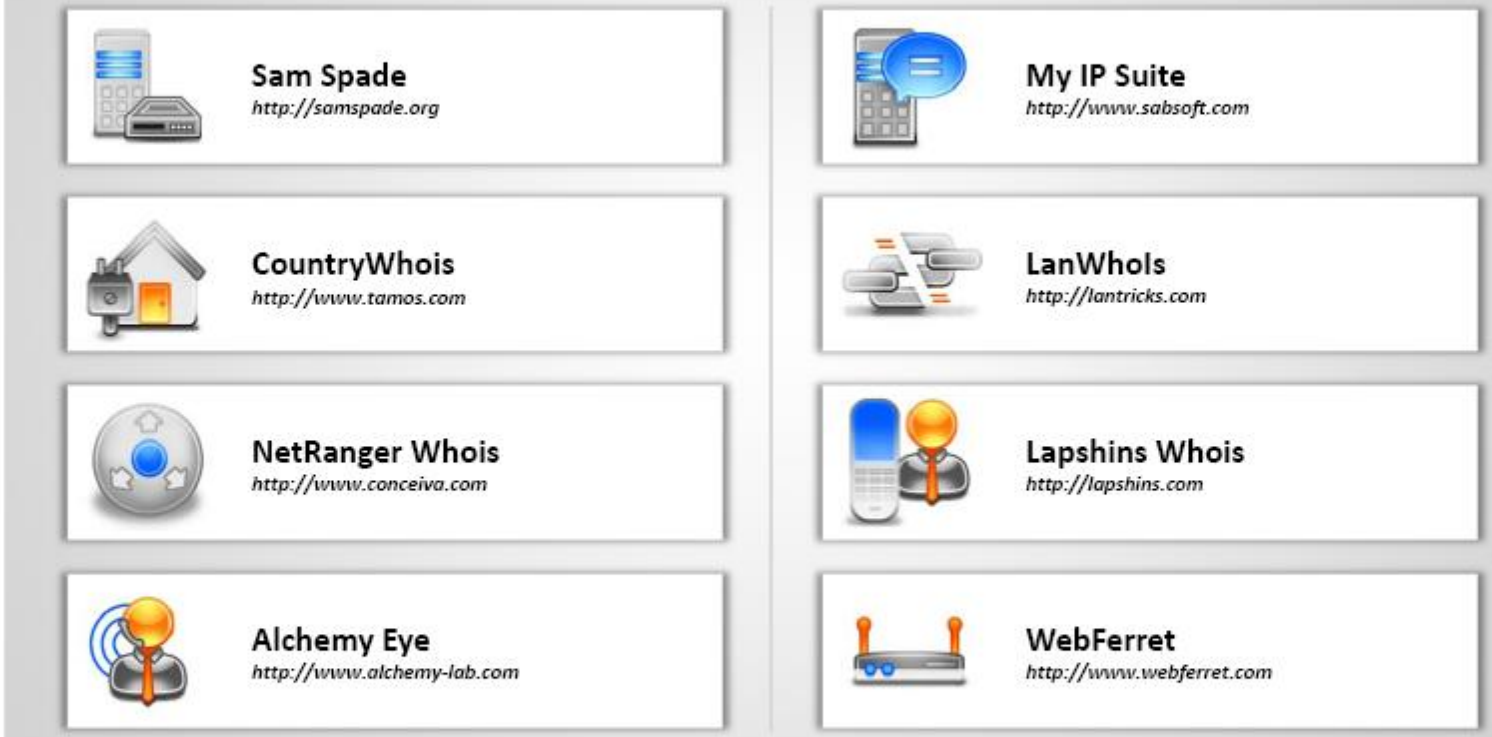
```
Domain servers in listed order:
    NS1.WEBHOST.COM              XXX.XXX.XXX.XXX
    NS2.WEBHOST.COM              XXX.XXX.XXX.XXX
```

# 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



# WHOIS Lookup Tools



# 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*

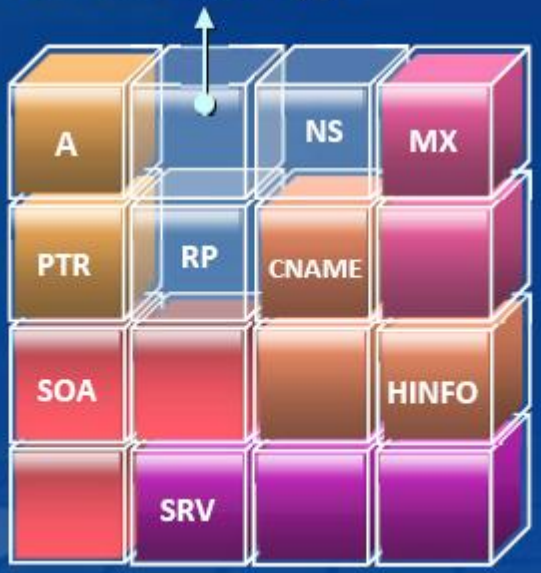
**DomainTools**
*http://www.domaintools.com*

**AutoWhois**
*http://centralops.net*

# Footprinting Methodology

# Extracting DNS Information

## DNS Record Type



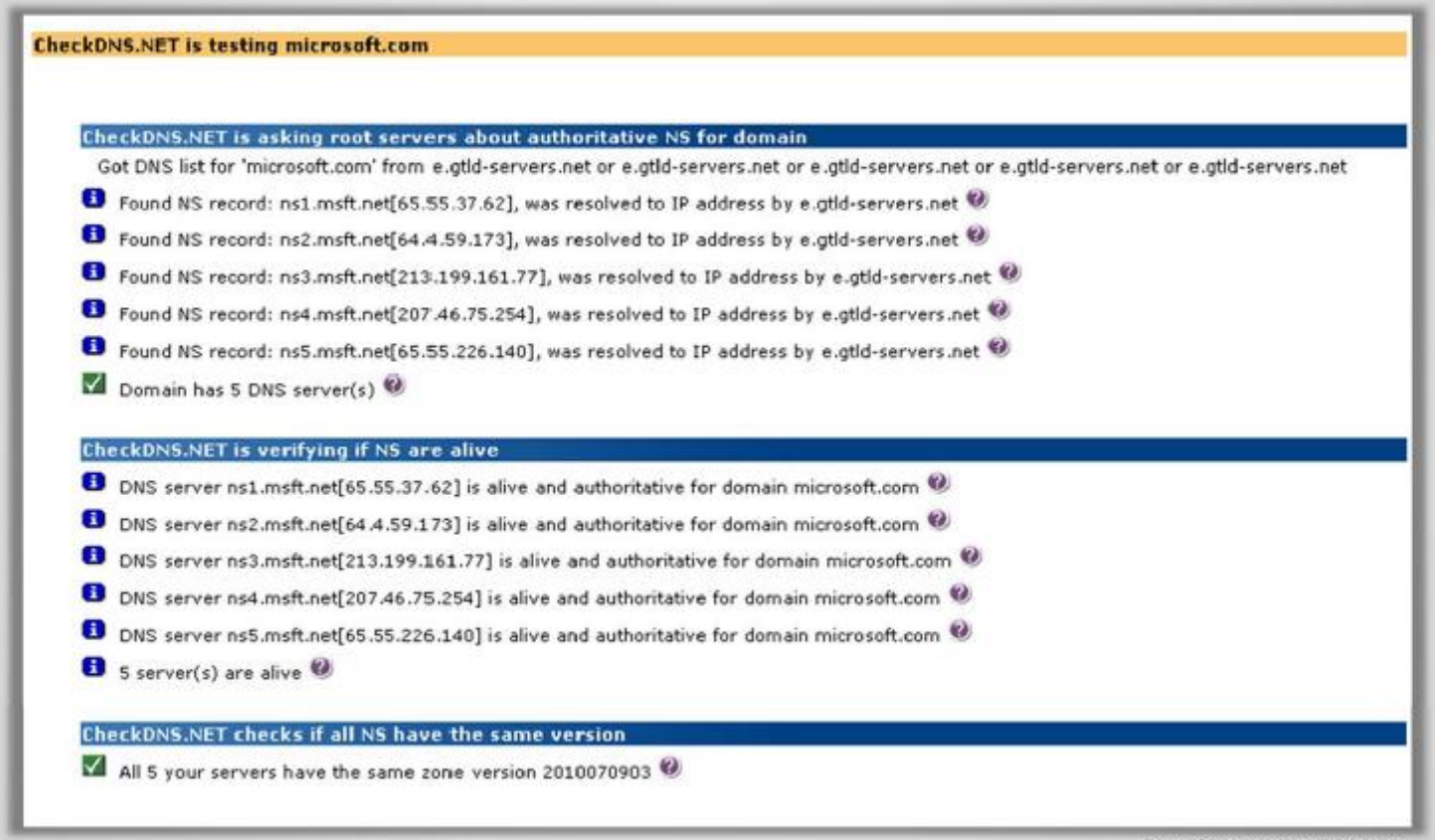

**DNS Records provide important information about location and type of servers**

- **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

# Extracting DNS Information




*http://www.checkdns.net*

# 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*

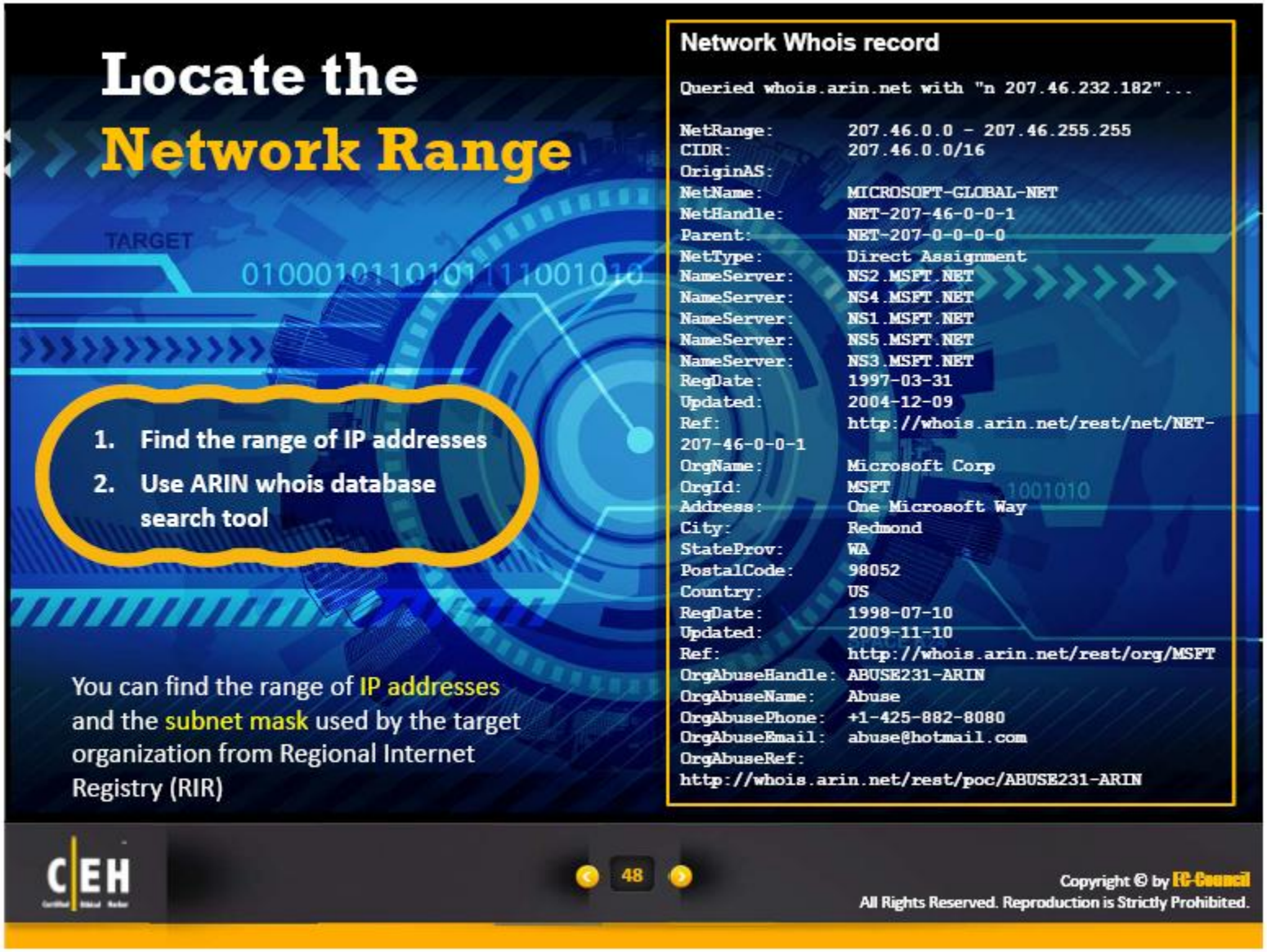
**Dnsmap**
*http://www.linuxhaxor.net*

**Multiple Addresses**
*http://www.checkdns.net*

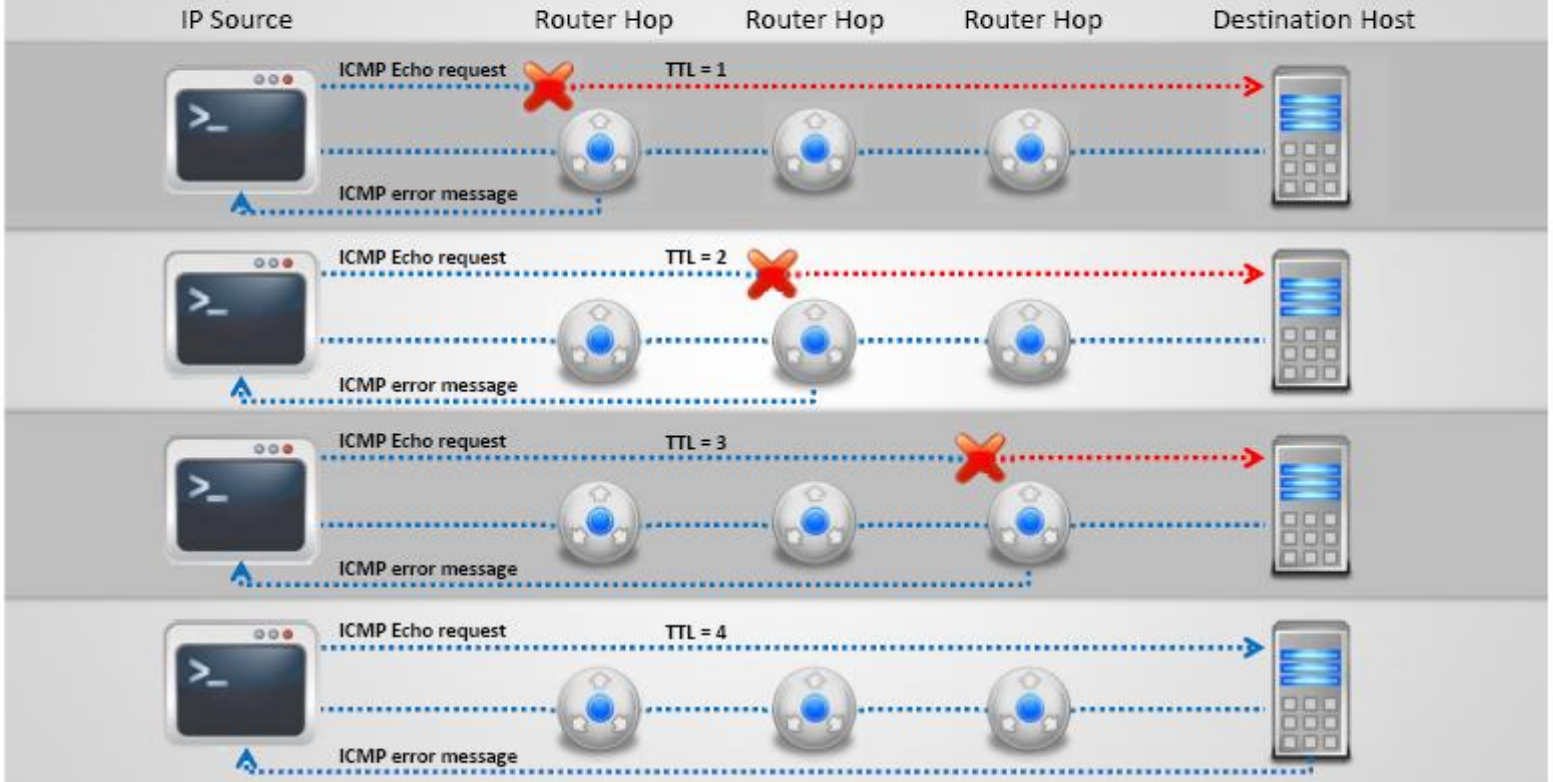
**DNS Tool**
*http://www.hendricom.com*

# DNS Interrogation Online Tools

# Footprinting Methodology



# 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

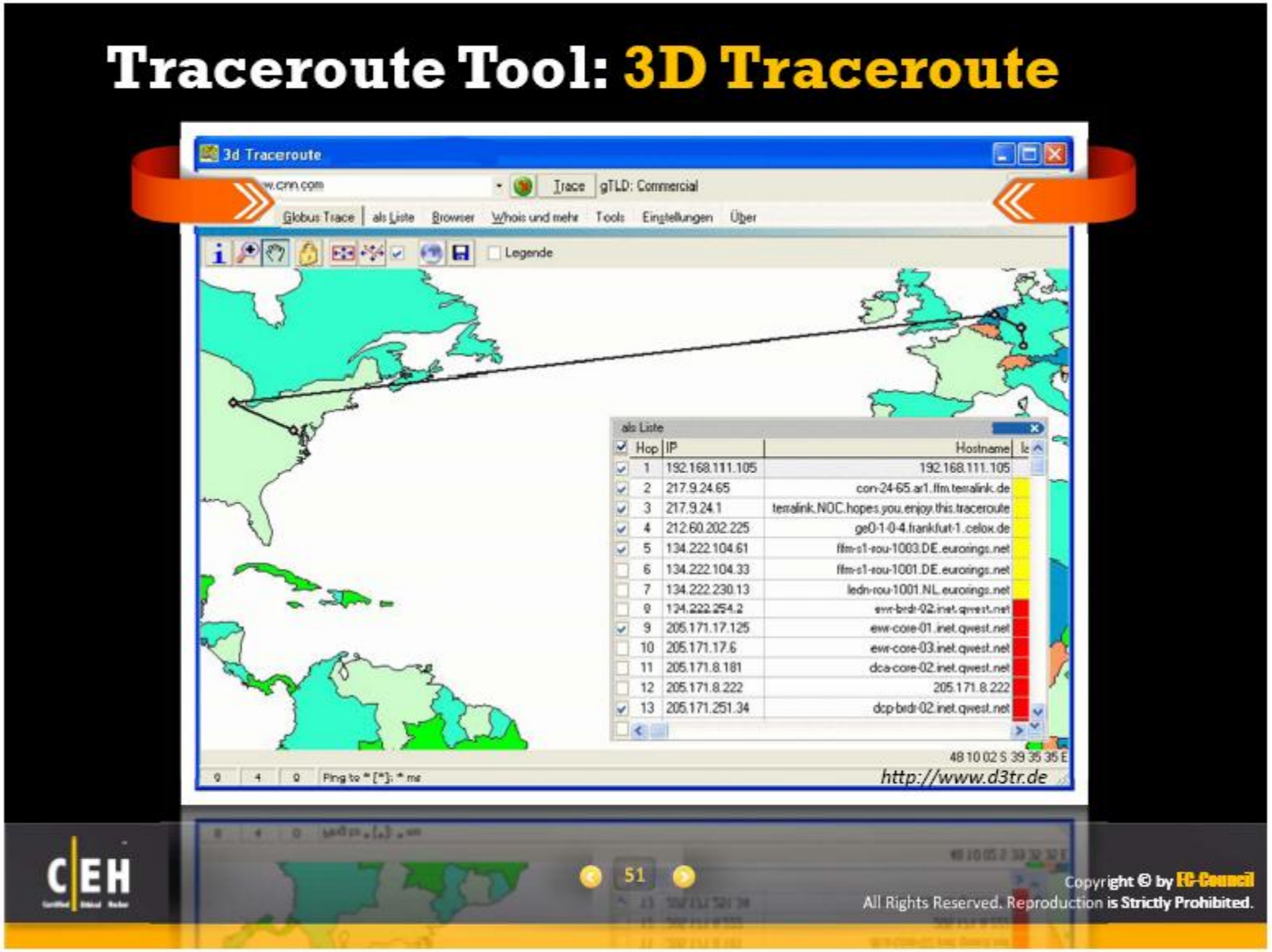
I Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations

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

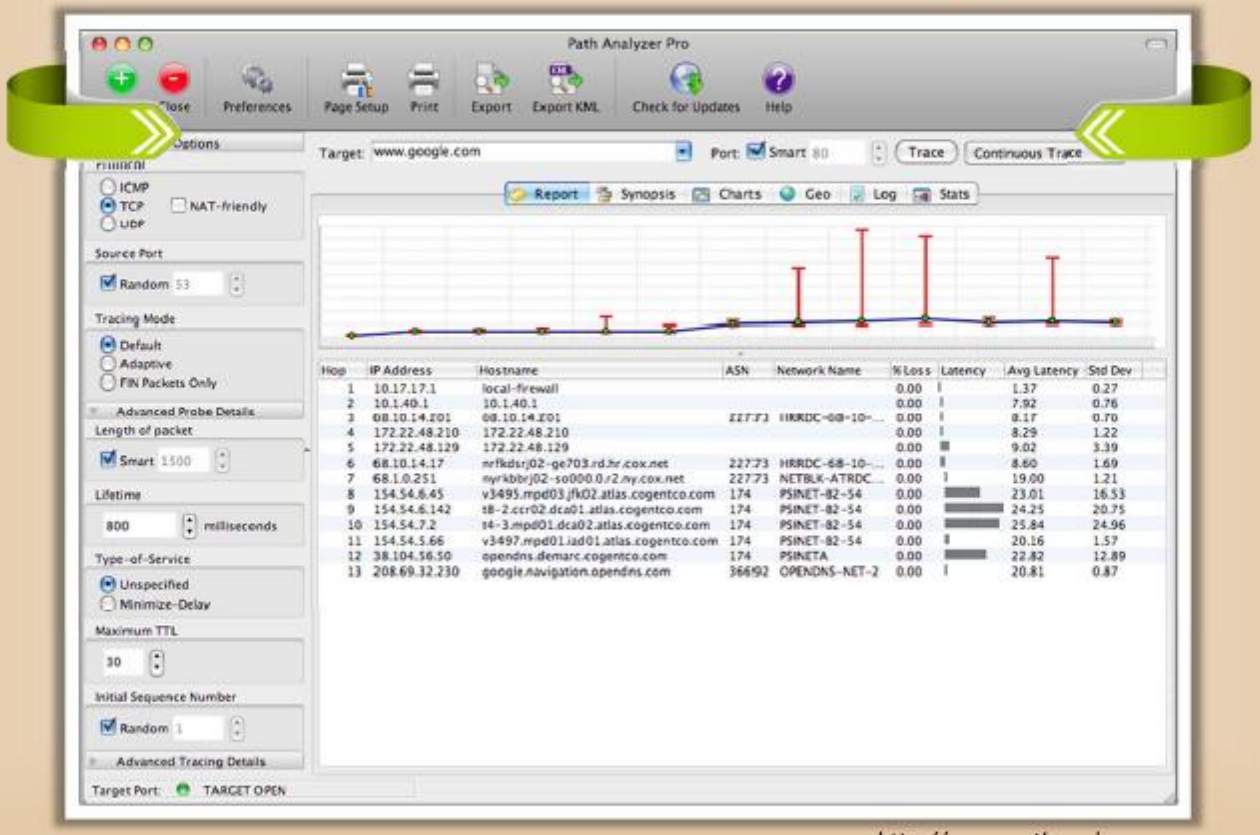
III By putting this information together, attackers can draw the network diagram

# Traceroute Tool: 3D Traceroute



# Traceroute Tool: LoriotPro

# Traceroute Tool: Path Analyzer Pro




http://www.pathanalyzer.com

# 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*

# 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

# 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*)

# 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*

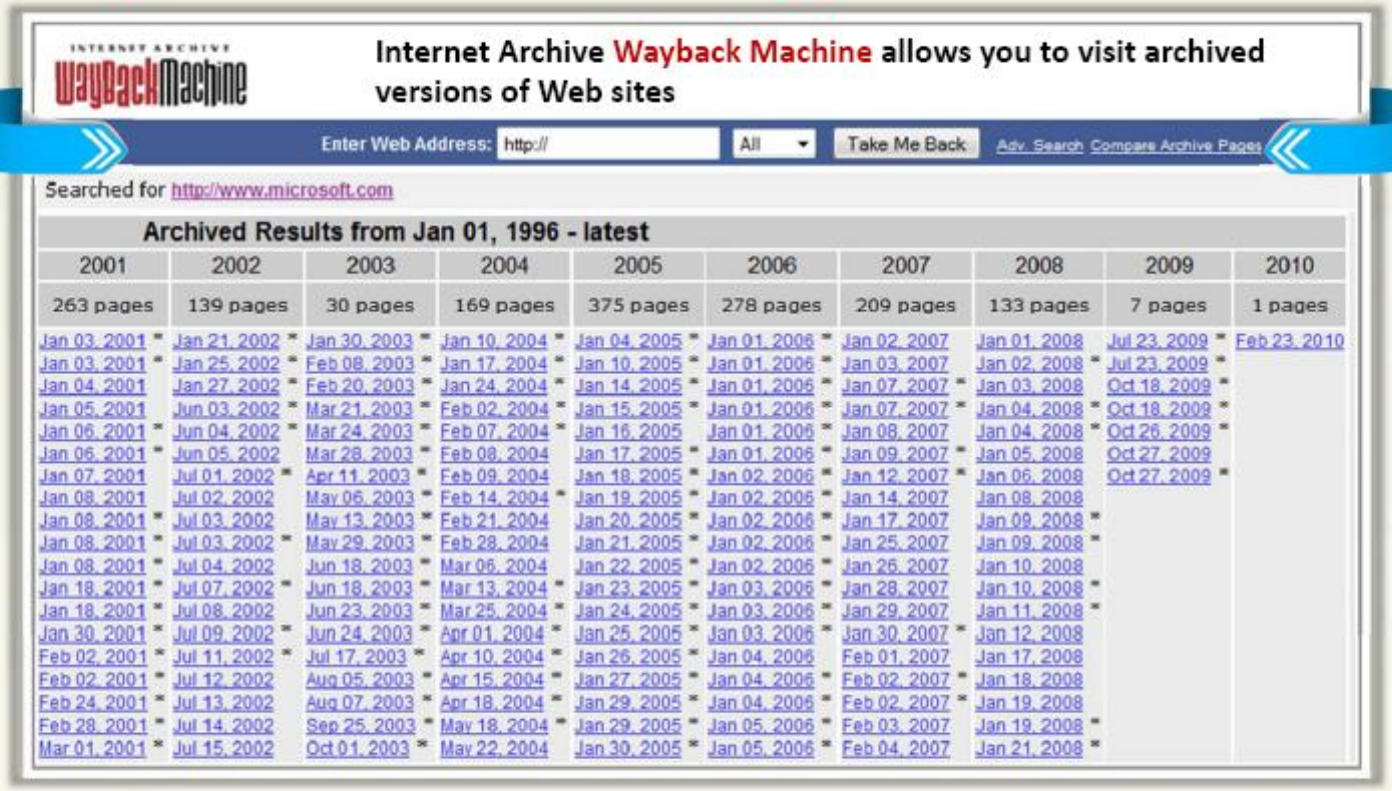
**WinWSD**
*http://winwsd.uw.hu*

**Reamweaver**
*http://reamweaver.com*

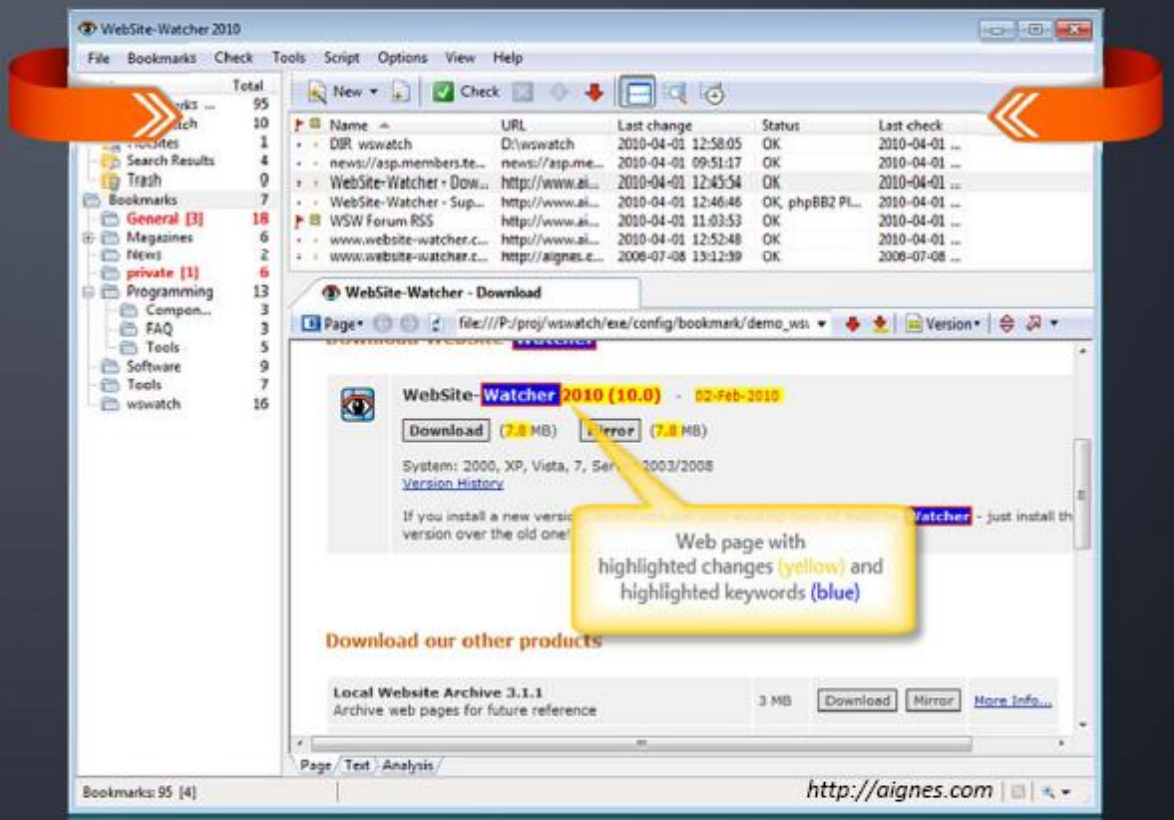
**xaldon webspider 2**
*http://www.xaldon.de*

**Teleport Pro**
*http://www.tenmax.com*

# Extract Website Information from http://www.archive.org



# Monitoring Web Updates Using Website Watcher



# Tracking Email Communications

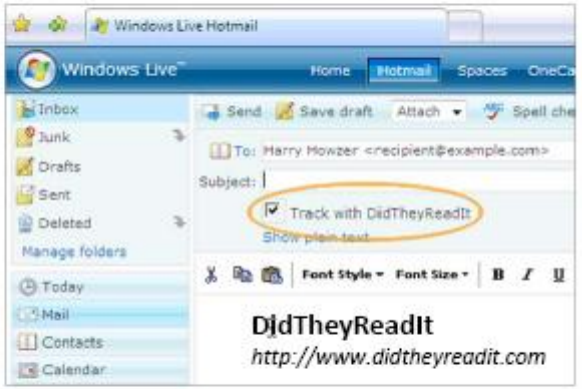
E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient

| | |
|---|---|
| 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 Tools

eMailTrackerPro
http://www.emailtrackerpro.com

Read Notify
http://www.readnotify.com


DidTheyReadIt
http://www.didtheyreadit.com

PoliteMail
http://www.politemail.com

# 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*

# Footprinting Methodology

# 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

# What a Hacker Can Do With Google Hacking?

# Google Advance Search Operators

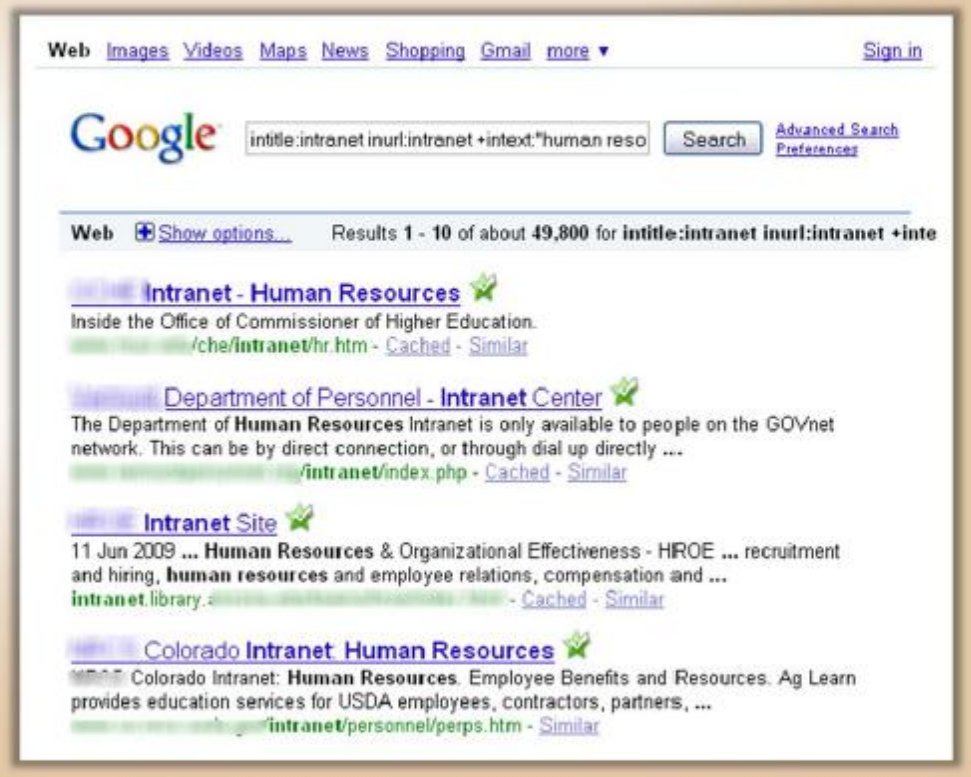
Google supports several advanced operators that help in modifying the search

| | |
|---|---|
| [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 Hacking Tool: Google Hacking Database (GHDB)

# Google Hacking Tools

**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*


Module Flow
Footprinting Concepts
Footprinting Threats
Footprinting Methodology
Footprinting Tools
Footprinting Countermeasures
Footprinting Pen Testing
CEH
73
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

# 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*

# 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*

# Additional Footprinting Tools

**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 Countermeasures

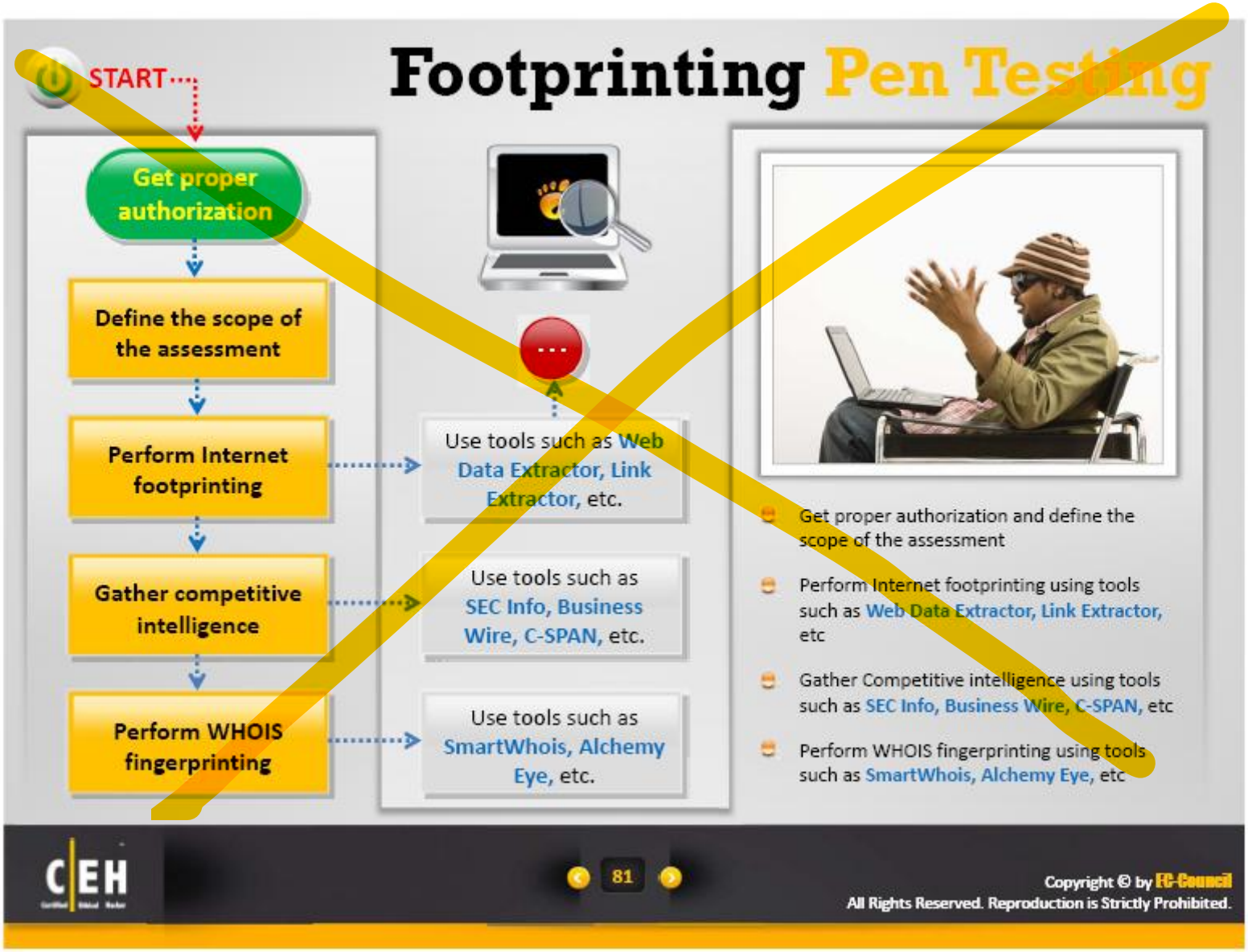
1. Configure routers to restrict the responses to footprinting requests
2. Configure web servers to avoid information leakage and disable unwanted protocols
3. Lock the ports with the suitable firewall configuration

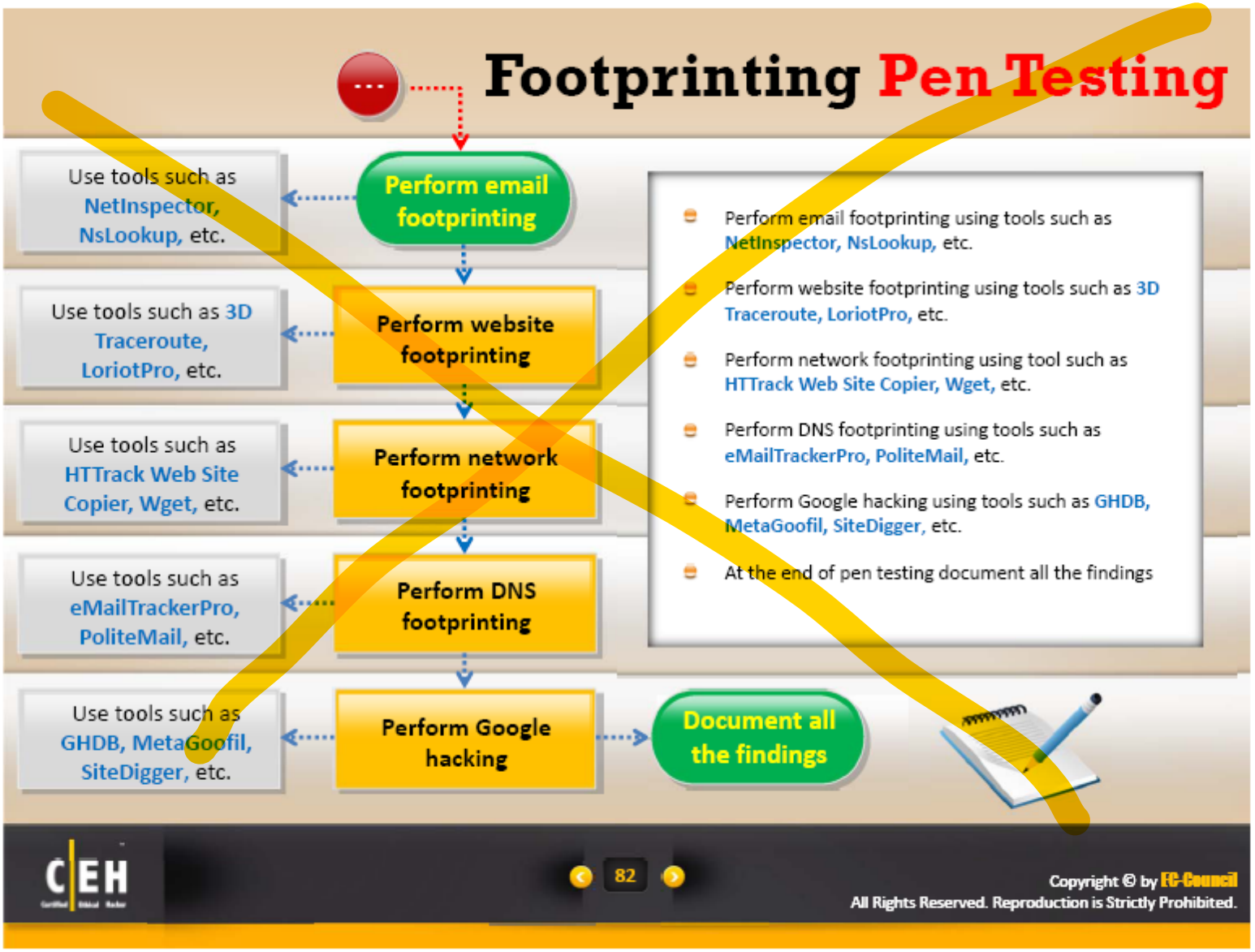

4. Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns
5. Evaluate the information before publishing it on the website/Internet

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

# 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**





# 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

# 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